BQN Guía Rápida
R4.0

Este documento le guiará en la puesta en marcha del dispositivo de optimización de tráfico Bequant BQN y describe sus principales funcionalidades.

1. Instalación

1.1. Requisitos

- **Dirección IP de gestión**, con su máscara y gateway para la ruta por defecto (ej. 10.10.1.47/24 con gateway 10.10.1.1).
- Cableado hacia la interfaz de red de **gestión RJ45**
- **Acceso remoto a la dirección IP de gestión** para los puertos TCP 22 (SSH) y 443 (HTTPS) desde la dirección IP de soporte de Bequant (46.26.190.166). Dicho acceso puede configurarse con reglas de reenvío de puertos en el router de acceso Internet.
- Cableado de tráfico de suscriptor: para cada pareja de interfaces de red, un cable o fibra desde el BQN al router/switch del lado de acceso y otro cable o fibra al router/switch del lado de Internet.
- Si se usan puertos de fibra de **10Gbps**, los tipos de transceptores soportados (deben ser compatibles con Intel, con las series X710 o X520) son:
    - SFP+ SR
    - SFP+ LR
    - SFP 1000Base SX o LX
- Si se usan puertos de **25Gbps**, los transceptores deben ser SFP28 y compatibles con Intel.
- Si se usan puertos de **40Gbps**, los transceptores tienen que ser QSFP+ y compatibles con la serie de Intel XL710.
- Si se usan puertos de **100Gbps**, los transceptores tienen que ser QSFP28 y compatibles con la serie de Intel E810.
- El encaminamiento del tráfico a través del BQN. Deberá hacerse **bidireccionalmente** (todo el tráfico de subida y bajada para los suscriptores seleccionados tiene que pasar por el BQN).
- Estándares de tráfico soportados IEEE 802.1Q (VLAN), IEEE 802.1ad (QinQ), IEEE 802.3ad (LACP), IETF RFC2516 (PPPoE), IETF RFC 3032 (MPLS).
- Esta guía supone que el software BQN está ya instalado. Si no fuera así, seguir primero la *Guía de Instalación del Software de Bequant*.

1.2. Pasos

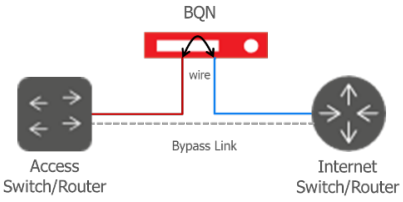
1. Conectar la alimentación y el puerto de gestión (ver en la sección *Servidores Soportados* los detalles exactos de su modelo de servidor).

2. Encender el servidor BQN y acceder a la GUI de gestión, siguiendo los pasos descritos en la sección de *Login* más adelante.

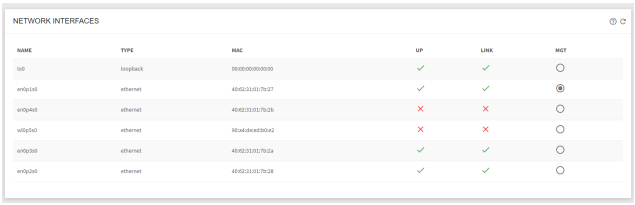
3. El BQN viene de fábrica con la dirección IP de gestión **192.168.0.121/24**, con **192.168.0.1** como *gateway* de la ruta por defecto**,** y con un usuario **`bqnadm`** de gestión con **contraseña** el **número de serie** (ver en la sección *Servidores Soportados* dónde se encuentra en su modelo).

4. Si necesita cambiar la dirección IP de gestión o el *gateway* de la ruta por defecto, véase la sección *Configuración Inicial*.

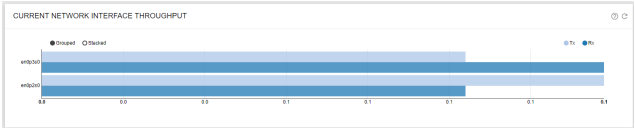
5. **Conectar los cables del tráfico de suscriptor**. Las interfaces de tráfico de suscriptor están emparejadas en *wires*, conectadas internamente de forma que el tráfico que entra por una interfaz es enviado por su pareja y viceversa. Para cada *wire* utilizado, hay que conectar una interfaz al lado de acceso y otra al lado de Internet. Es importante conectar las interfaces a su lado correcto (de lo contrario, se afectará al rendimiento del sistema). Ver en la sección *Servidores Soportados* los detalles exactos de su modelo de servidor.



6. Las interfaces de red en uso deben estar arriba y con enlace detectado. Ambas cosas son monitorizables en la GUI en *Status->Interfaces->Link State*.



7. Una vez se hace pasar tráfico, se puede ver su valor instantáneo en la opción *Status->Interfaces->Throughput*.



8. Y eso es todo. La instalación ha finalizado.

2. Servidores Soportados

A continuación, se listan algunos de los modelos de servidor soportados.

En los diagramas que siguen se numeran las interfaces de red para facilitar las instrucciones de cableado, empezando por el 1 para la interfaz de gestión. La correspondencia de las interfaces físicas con las mostradas en la GUI puede establecerse conectando una interfaz física cada vez y comprobando en *Status->Interfaces->Link State* cuál de las interfaces pasa a tener su estado de enlace arriba.

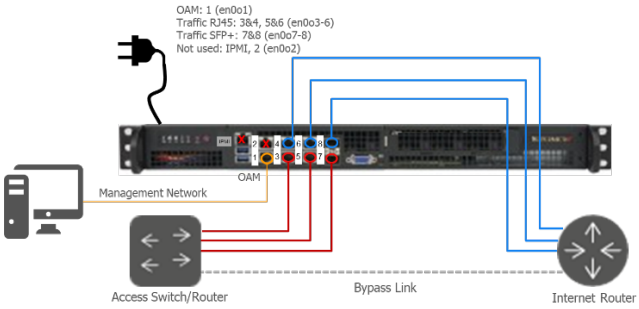
Las interfaces de tráfico de suscriptor se emparejan en *wires*, con la interfaz en el lado de acceso listada primero y seguidamente la del lado de Internet.

Por ejemplo, en el *wire* 3&4, la interfaz 3 está en el lado de acceso y la 4 en el lado de Internet.

2.1. Supermicro

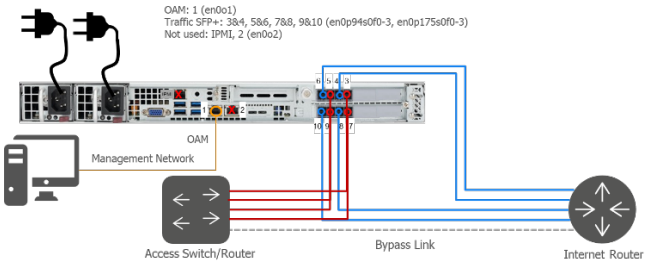
El **número de serie** es un valor alfanumérico de quince caracteres impreso en una etiqueta en la parte posterior izquierda.

SM SuperServer 5018D-FN8T



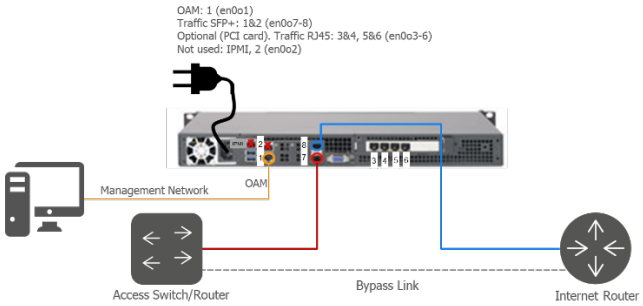
La interfaz 1 (inferior izquierdo) es la de gestión. Los *wires* son 3&4 (RJ45), 5&6 (RJ45) y 7&8 (SFP+). Las interfaces 2 y IPMI no se usan.

SM SuperServer 1029P-WTR



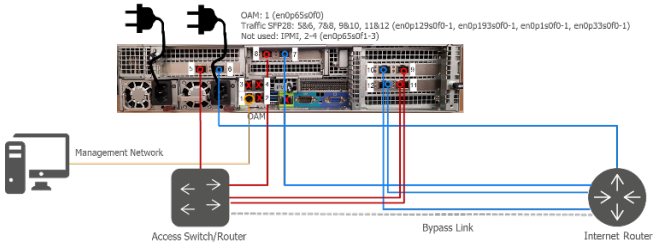
La interfaz 1 (inferior izquierda) es la de gestión. Los *wires* son SFP+, emparejados en interfaces contiguas, con la de acceso a la derecha del par. Las interfaces 2 y IPMI no se usan.

SM SuperServer 5018D-LN4T



La interfaz 1 (inferior izquierda) es la de gestión. El *wire* de SFP+ es entre las interfaces integradas 7&8. Opcionalmente, se puede instalar una tarjeta PCI. En la figura se usa una de cuatro puertos RJ45 para establecer dos wires 3&4 y 5&6. Las interfaces 2 y IPMI no se usan.

SM SuperChassis 829BTQ-R920WB

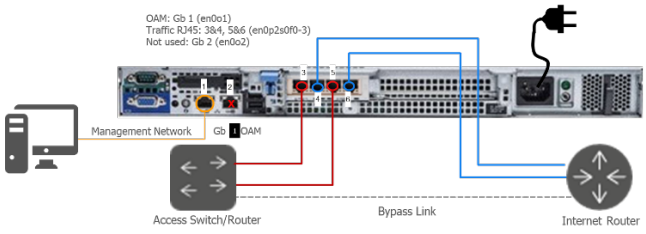


La interfaz 1 (inferior izquierda) es la de gestión. Los wires son cada una de las parejas de puertos de las tarjetas PCI (puertos de 25 Gbps).

2.2. Dell

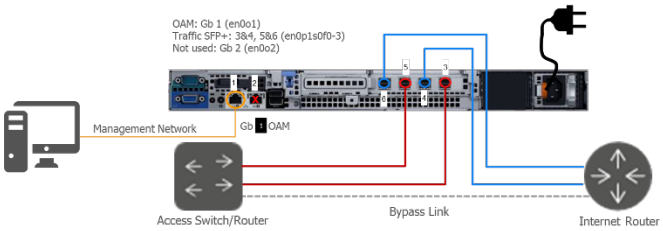
El **número de serie** es un valor alfanumérico de siete caracteres, impreso en una pestaña extraíble en el frontal del servidor, identificado como “Service Tag”.

Dell PowerEdge R230



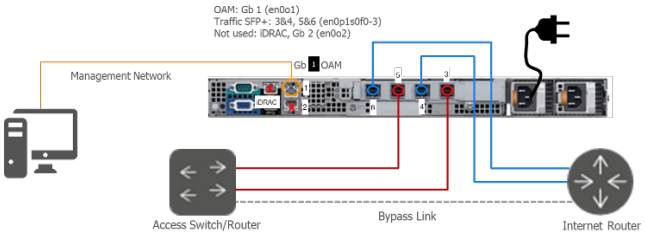
La interfaz 1 (Gb 1) es la de gestión. Los *wires* disponibles dependen de la tarjeta configurada. En el ejemplo, se usa una tarjeta de cuatro puertos RJ45. La interfaz 2 (Gb 2) no se utiliza.

Dell PowerEdge R330



La interfaz 1 (Gb 1) es la de gestión. Los *wires* disponibles dependen de la tarjeta configurada. En el ejemplo, se usa una tarjeta de cuatro puertos SFP+. La interfaz 2 (Gb 2) no se utiliza.

Dell PowerEdge R440

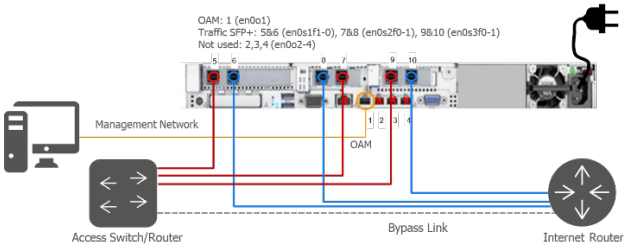


La interfaz 1 (Gb 1) es la de gestión. Los *wires* disponibles dependen de la tarjeta configurada. En el ejemplo, se usa una tarjeta de cuatro puertos SFP+. Las interfaces 2 (Gb 2) e iDRAC no se utilizan.

2.3. HPE

El **número de serie** es un valor alfanumérico de diez caracteres, impreso en una pestaña extraíble en el frontal del servidor, identificado como “S/N”.

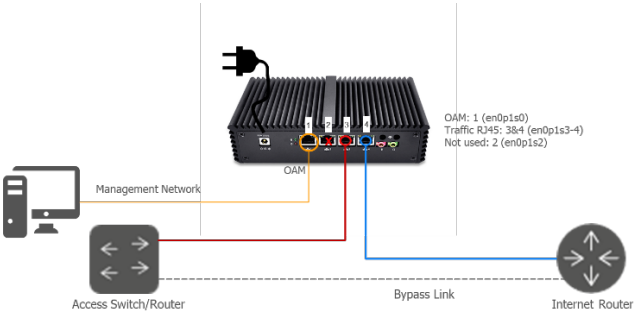
HPE Proliant DL360



La interfaz 1 es el de gestión. Los *wires* disponibles dependen de la tarjeta configurada. En el ejemplo, se usan tres tarjetas de dos puertos SFP+ cada una. Las interfaces 2, 3, 4 e iLO no se utilizan.

2.4. Plataforma HW *Fanless*

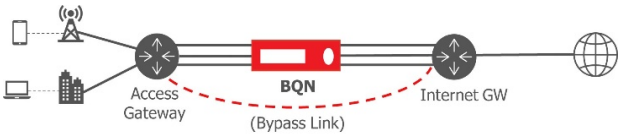
El número de serie es un valor alfanumérico de diez caracteres impreso en la parte de abajo.



La interfaz 1 es la de gestión. El *wire* disponible es el 3&4 (RJ45). La interfaz 2 no se utiliza.

3. Despliegue en la Red

La mayor parte de la funcionalidad del BQN necesita visibilidad de las IPs de cada suscriptor (por ejemplo, para limitar la velocidad máxima de cada uno de ellos). Por este motivo, es importante desplegar el BQN en una posición de la red donde no haya un NAT entre el BQN y los suscriptores.



Se recomienda un camino de *bypass* entre los nodos adyacentes al BQN (Access e Internet Gateways en la figura sobre estas líneas), de forma que, si hay un fallo en el enlace activo o en el propio BQN, el tráfico se conduzca automáticamente a través del *bypass*. Dicho *bypass* se puede establecer en capa 2 (ej. mediante el bonding de enlaces *active-backup* de Mikrotik o de un grupo LACP) o en capa 3 (ej. enrutado dinámico por OSPF o BGP). Al tratarse de enlaces directos entre los dos extremos, de forma transparente con el BQN en medio, la detección de fallos de los enlaces no debe ser eléctrica (ej. MII), sino basada en mensajes (ej. ARP or fast LACP).

4. Introducción a la GUI

El BQN tiene una interfaz gráfica (GUI) web desde la que se pueden hacer las tareas de gestión más comunes. Se soportan los navegadores para desktop de Chrome, Firefox, Safari y Microsoft Edge (MS Explorer no está soportado).

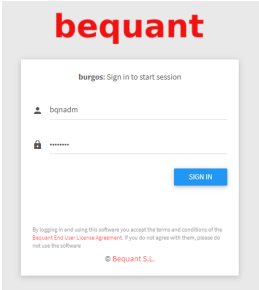
La GUI tiene ayuda contextual: presione el icono (?) en la página en la que se necesita ayuda.

4.1. Login

Para acceder a la GUI, abrir un navegador y visitar la URL: **`https://`*`oam-ip`***, donde *oam-ip* es la dirección IP de gestión (192.168.0.121 de fábrica).

El BQN usa un certificado autofirmado y el navegador lo indicará como inseguro. Ignorar la advertencia e ir a la página web.

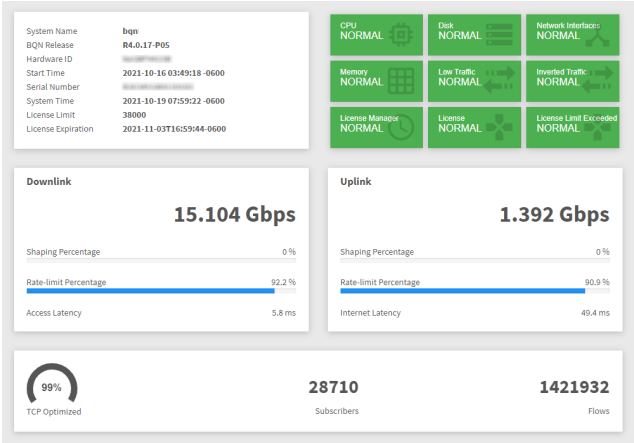
Introducir el usuario `bqnadm` y la contraseña (por defecto, el número de serie del servidor).



El usuario `root` no puede usarse para entrar en la GUI.

4.2. Página de Inicio. *Dashboard*

La página de inicio tiene un menú lateral, un tablero de estado (*dashboard)* y un pequeño resumen de información de sistema.

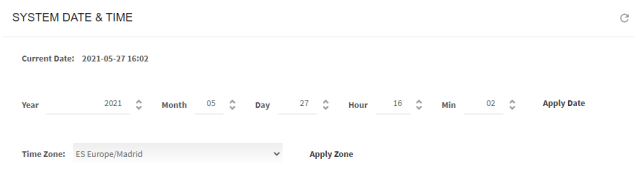


El *dashboard* debe estar con todos los iconos en verde. El icono *NETWORK INTERFACES* no estará en verde hasta que se conecten los puertos de datos (si hay interfaces sin uso en alguno de los *wires* configurados, permanecerá en naranja) y el icono TRAFFIC no estará en verde hasta que pase tráfico por ellos. En algunos iconos, pulsar en ellos lleva a una ventana donde obtener más información sobre el estado del BQN.

5. Configuración Inicial

5.1. Cambiando la hora

Si es necesario cambiar la hora del sistema, seleccionar *Administration->System Date->Ser Date & Time*.



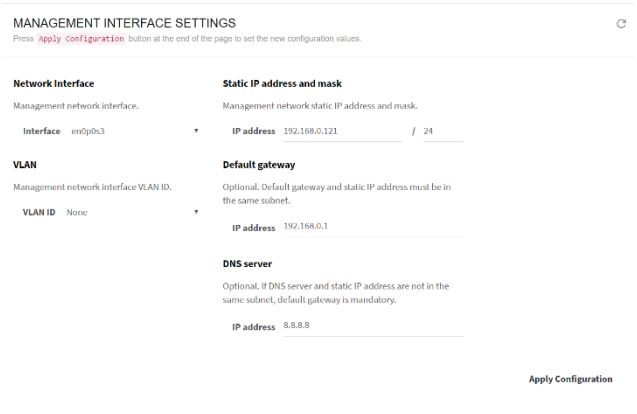
Apply Data cambia la fecha y hora locales y *Apply Zone* la zona horaria. Es posible navegar la lista de zonas horarias pulsando en el teclado las iniciales del país al que se quiere ir (ej. ES para España).

5.2. Cambiando la dirección IP de Gestión

Para **cambiar la dirección IP**, seleccionar en el menú lateral izquierdo la opción *Configuration->Interfaces->Management*. La configuración incluye la dirección IP y máscara de red (*Static IP address and mask*), la pasarela por defecto (*Default gateway*) y el identificador de VLAN (en caso de haberlo). La pasarela por defecto no es obligatoria, pero se recomienda configurarla.

Opcionalmente se puede definir la dirección IP de un servidor DNS.

El puerto de red de gestión (*Network Interface*) no debe cambiarse a menos que lo indique el soporte de Bequant.



Cuando se complete la nueva configuración, se presiona *Apply Configuration* para aplicar los cambios. Para conectarse de nuevo al servidor hay que acceder desde la nueva subred y logarse otra vez a la GUI.

5.3. *Firewall* para la Interfaz de Gestión

Para **configurar el *firewall* de la interfaz de gestión**, (que aplicará sólo a la interfaz de gestión, no a las interfaces de tráfico de suscriptores), seleccionar en el menú lateral *Configuration->Interfaces->Management Firewall*. Se mostrará los rangos de direcciones IP a los que se permite el acceso a la interfaz de gestión. Por defecto, no habrá ningún rango configurado y ninguna dirección IP será bloqueada.

Para añadir un rango de direcciones permitidas, pulsar el icono ⋮ y seleccionar *Add IP Address Range…*. El *firewall* se activa al introducir un rango de direcciones, quedando bloqueadas todas las direcciones IP que no estén dentro de los rangos configurados. Conviene por tanto que el primer rango de direcciones que se introduzca incluya a la dirección IP desde la que se está operando la GUI. También debería incluirse la subred que incluye la dirección IP de la interfaz (la GUI nos avisará si esto no se cumple).

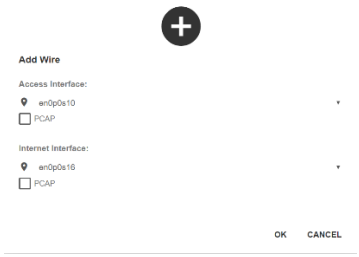
5.4. Configuración de *Wires*

Un *wire* es una pareja de interfaces de red que procesan tráfico de usuarios y que funcionan como un *bridge*.

Para configurar *wires*, hay que ir a la opción *Configuration->Interfaces->Data Wires*.

Los wires son direccionales, con la primera interfaz de red conectada al lado del acceso de los suscriptores y la segunda interfaz al lado de Internet. Si se ha producido un error en el conexionado se pueden intercambiar los puertos pulsando el icono ⇆.

Para añadir un *wire*, pulsar el icono ⋮ y seleccionar *Add Wire…*. Se mostrará un formulario donde especificar las interfaces de acceso e Internet (el formulario listará las disponibles). La opción `pcap` se selecciona únicamente en el caso de tarjetas que nos sean de las series de Intel I350, X520, X710 o XL710 (`pcap` permite la compatibilidad al precio de reducir el rendimiento del servidor).



Para eliminar un *wire*, se pulsa el icono 🗑.

No se debe eliminar un *wire* a menos que así lo indique el soporte de Bequant, ya que un error puede dar lugar a pérdida de servicio.

Los cambios sólo se aplican al clicar *Apply Configuration*.

6. Funcionalidades del BQN

El BQN permite realizar las siguientes funciones sobre el tráfico que fluye por él:

- Optimización TCP (TCPO).
- Limitación de velocidad de ciertas aplicaciones por suscriptor (*shaping*).
- Bloqueo de ciertos tipos de tráfico.
- Limitación de la velocidad total de cada suscriptor (gestión de planes).
- Detección de ataques de DoS.
- Métricas de tráfico por suscriptor y por servicio.

6.1. Conceptos Básicos de la Configuración

Todos los paquetes de datos IP que atraviesan el BQN pertenecen a un suscriptor y a un flujo. El BQN actúa sobre el tráfico así agrupado en suscriptores y flujos.

- Un **suscriptor** es una dirección IPv4 en el lado de acceso, o una dirección IPv6 del lado de acceso de la misma subred /64. Ver la sección *Identificación de Suscriptores* para más detalles.
- Un **flujo** es una conexión TCP, o una conexión UDP o una conexión de otro protocolo IP (ej. ping ICMP).

Un suscriptor tiene uno o varios flujos al mismo tiempo.

Para decidir las funcionalidades a aplicar a cada tráfico (sea un suscriptor o un flujo), el BQN aplica tres conceptos: políticas, perfiles y reglas.

- Las **políticas** definen las acciones a aplicar al tráfico, junto con los parámetros de las acciones (ej. un límite de velocidad).
- Los **perfiles** clasifican el tráfico de acuerdo con algún criterio (por ejemplo, un perfil de acceso identifica el tráfico de todos los suscriptores cuya dirección IP está contenida en el conjunto de rangos de direcciones IP de ese perfil de acceso).
- Las **reglas** relacionan perfiles y políticas. Por ejemplo, una regla puede especificar que cierto perfil de acceso esté limitado por una política de caudal por suscriptor, es decir, que los suscriptores cuya dirección IP esté en ciertas subredes tendrán un límite de velocidad determinado.

6.2. Perfiles

Los perfiles clasifican el tráfico y especifican, junto con las reglas, qué políticas se aplican a los suscriptores y a los flujos al que aplicar una política. Hay distintos tipos de perfiles de tráfico según las propiedades utilizadas en su clasificación, y pueden definirse más de un perfil de cada tipo. En la versión actual son los siguientes:

- **Perfil de Interfaz (*Interface*)**: identifica a todos los flujos o suscriptores cuyo primer paquete de datos entra por una interfaz incluida en la lista de interfaces de red de dicho perfil.
- **Perfil de VLAN**: identifica a todos los flujos o suscriptores cuyo primer paquete de datos tiene una etiqueta de VLAN incluida en la lista de etiquetas de VLAN de dicho perfil.
- **Perfil de Internet**: identifica a todos los flujos que van a, o vienen de, una dirección IP del lado de Internet, contenida en la lista de rangos de direcciones IP de dicho perfil. Opcionalmente, también se pueden especificar puertos del lado de Internet (ej. puerto 80).
- **Perfil de Acceso (*Access*)**: identifica a todos los flujos que van a, o vienen de, una dirección IP del lado de Acceso, contenida en la lista de rangos de direcciones IP de dicho perfil de acceso. Opcionalmente, también se pueden especificar puertos del lado de acceso.
- **Perfil de DPI (*Deep Packet Inspection*)**: identifica a todos los flujos que utilizan un dominio HTTP/HTTPS/QUIC incluido en la lista de dominios HTTP/HTTPS/QUIC de dicho perfil. Hay un conjunto de firmas DPI predefinidas, que incluyen los dominios de aplicaciones populares (como las más importantes aplicaciones de video-streaming o las actualizaciones de software más comunes).

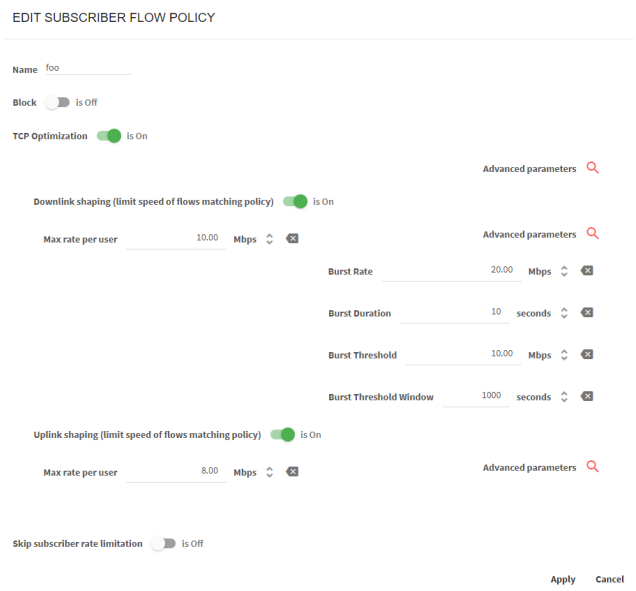
- **Perfil de Caudal (*Throughput*)**: identifica a todos los flujos que han sido creados en un momento en el que el caudal total de tráfico de bajada atravesando el BQN estaba por encima del umbral especificado por dicho perfil.

Los perfiles se configuran en la opción de menú *Configuration->Profiles*.

6.3. Políticas de Flujo por Suscriptor (*Subscriber Flow Policies*)

Cuando un nuevo flujo es creado, se le asigna una política de flujo por suscriptor, que tratará todos los flujos dentro de ese suscriptor confirme a esa política. Las acciones que se pueden definir en una política de flujo por suscriptor son:

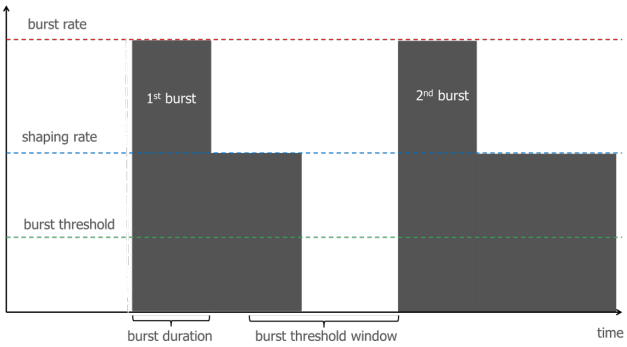
- **Optimización TCP**. Mejora el rendimiento del tráfico TCP. Se especifica si aplicar o no optimización TCP. Se recomienda hacerlo (el valor por defecto)
- **Limitación de velocidad de aplicaciones** (*Shaping*). Se limita el caudal a ese valor. Se puede limitar en la dirección de subida (*uplink*) y/o bajada (*downlink*). La limitación se aplica al conjunto de flujos que caen dentro de cada política y que pertenecen a un mismo suscriptor. Por ejemplo, si se especifica un límite de 6 Mbps para los contenidos de *streaming* de vídeo, y el cliente tiene 3 flujos de *streaming* de vídeo, los 3 flujos se repartirían el límite de 6 Mbps (obteniendo cada uno 2 Mbps, en principio). Es posible definir ráfagas (*bursts*) que permitan a los flujos exceder este límite temporalmente (véase al final de esta sección).
- **Bloqueo** (*Block*). Bloquea ese tipo de tráfico y no lo deja pasar. Debe usarse con cuidado, para evitar afectar un tráfico distinto al deseado.
- **Sin límite por Política de Caudal** (*Skip subscriber rate limitation*): Libera a estos flujos de cualquier límite que haya definido a nivel de Caudal de Suscriptor.



Estas políticas se configuran en la opción de menú *Configuration->Subscriber Flows*, entrando en la pestaña *POLICIES*.

Con relación a las **ráfagas o *bursts***, se configuran en los *Advanced parameters* de la dirección adecuada (ej. *Downlink shaping*). La política de ráfagas la definen cuatro parámetros:

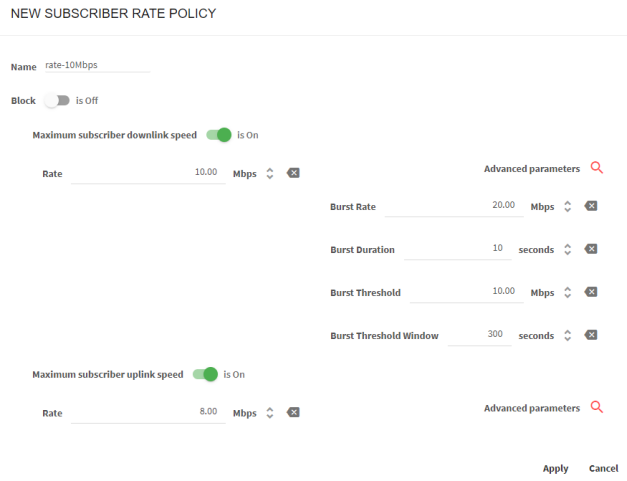
- *Burst Rate*: es la velocidad máxima durante la ráfaga, normalmente mayor a la velocidad del shaping (ej. permitir ráfagas de 20 Mbps para flujos normalmente limitados a 10 Mbps).
- *Burst Duration*: duración de la ráfaga, es decir, durante cuánto tiempo puede sostenerse.
- *Burst Threshold*: es la velocidad media que, de excederse, impide que se pueda tener una nueva ráfaga. Es la manera de controlar cuándo se concede una nueva ráfaga. Por ejemplo, para un límite de 10 Mbps con ráfagas de 20 Mbps, un umbral de 5 Mbps requiere que el suscriptor baje su velocidad a la mitad de su límite normal, antes de que le conceda una nueva ráfaga.
- *Burst Threshold Window*: es el periodo, en segundos, usado para computar la velocidad media a chequear contra el umbral. Cuanto mayor la duración de la Ventana, mayor será el peso de la actividad pasada del suscriptor en la concesión de una nueva ráfaga.



6.4. Políticas de Caudal por Suscriptor (*Subscriber Rate Policies*)

Estas políticas de velocidad se aplican por suscriptor. Las acciones posibles en una de estas políticas son:

- **Máxima velocidad de bajada** (*Maximum subscriber downlink speed*). La máxima velocidad de bajada de todo el tráfico hacia la dirección IP del suscriptor. Se pueden configurar ráfagas, con idénticos parámetros que las de políticas de flujo, sólo que aplicadas a la política de caudal. Ver el final de la sección 6.3 para más detalles.
- **Máxima velocidad de subida** (*Maximum subscriber uplink speed*). La máxima velocidad de subida de todo el tráfico hacia la dirección IP del suscriptor. Se pueden configurar ráfagas, con idénticos parámetros que las de políticas de flujo, sólo que aplicadas a la política de caudal. Ver el final de la sección 6.3.
- Bajo *Advanced Parameters*, existen las mismas opciones de ráfaga ya descritas para las políticas de flujo por suscriptor.



Estas políticas se configuran en la opción de menú *Configuration->Subscriber Rates*, entrando en la pestaña *POLICIES*.

Ver en la sección, *Identificación de un Suscriptor*, cómo se identifica el tráfico de un mismo suscriptor.

> Las políticas de caudal por suscriptor también se pueden crear dinámicamente por medio de las APIs del BQN (RADIUS y REST). En ese caso, los parámetros de las políticas y los suscriptores asociados a ellas se controlan desde el API y son independientes de las reglas configuradas en el BQN (las reglas configuradas actúan de respaldo para suscriptores sin política via el API).

6.5. Reglas

Las reglas especifican qué políticas se asignan a cada suscriptor y flujo, en función de cómo satisfacen los perfiles de dichas reglas.

Hay un conjunto de reglas independientes por cada tipo de política: las reglas de flujo por suscriptor seleccionan la política de flujo (*Subscriber Flow*) apropiada para los flujos de un suscriptor, las reglas de caudal por suscriptor, la política de caudal (*Subscriber Rate*) y, por último, las reglas de monitorización por suscriptor determinan la política de monitorización (*Subscriber Monitoring*).

Una regla puede utilizar un solo perfil de cada tipo (o alternativamente, la opción *any* si ese tipo de perfil le es indiferente), y define una y solo una política a aplicar.

Cada conjunto de reglas puede tener varias reglas, pero solo una regla es la mejor coincidencia y será la elegida. Para evaluar las reglas de un modo que maximice el rendimiento, los perfiles se comprueban en orden. Este orden predefinido determina qué regla se elige finalmente. Una vista en árbol de las reglas ayuda a identificar la regla seleccionada en cada caso. Ver las secciones de *Árbol de Decisión* para ver detalles de dichos árboles y del orden de evaluación de los perfiles.

No se usan prioridades de regla configuradas manualmente por las penalizaciones de rendimiento que implican y porque cargan al operador con la responsabilidad de mantener consistentes las prioridades.

Las reglas de flujo por suscriptor se configuran en la opción del menú *Configuration-> Subscriber Flows*, entrando en la pestaña *RULES TREE-VIEW* o *RULES TABLE-VIEW*. Análogamente, las reglas de caudal por suscriptor en *Configuration->Subscriber Rate* y las

reglas de monitorización por suscriptor en *Configuration->Subscriber Monitoring*.

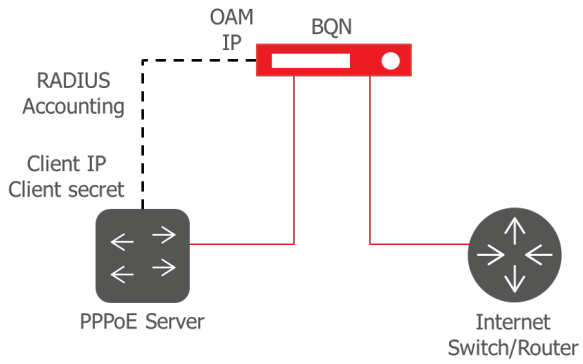
6.6. APIs

El BQN tiene dos APIs para seleccionar la política de caudal para suscriptor, en vez de usar las reglas locales del BQN, que actúan como opciones por defecto. Hay dos APIs, RADIUS y REST.

RADIUS

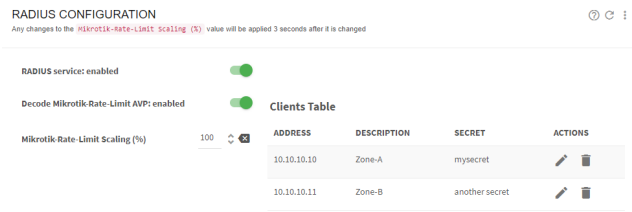
En el caso de las políticas de caudal por suscriptor, cual es seleccionada puede hacerse mediante señalización RADIUS en vez de mediante reglas.

Cuando se recibe señalización RADIUS indicando que a un suscriptor con una cierta IP le corresponde una política, se selecciona dicha política con independencia de lo que determinen las reglas configuradas, que aplican solo para suscriptores para los que no se ha obtenido ninguna información vía RADIUS.



El BQN recibe la información de RADIUS *accounting*, configurando la fuente del RADIUS (ej. un servidor PPPoE o un servidor RADIUS) para que envíe dicha información a la IP de gestión del Bequant.

En el Bequant hay que ir a *Configuration->RADIUS*, habilitar RADIUS (*Radius is On*) y seleccionar en el menú superior derecho *Add Client…* para configurar la IP de la fuente del RADIUS *accounting* y el secreto (*secret*) que utiliza. Es posible configurar más de una fuente.



Ahora mismo, los campos RADIUS soportados son los *Address List* y *Rate Limit* de Mikrotik.

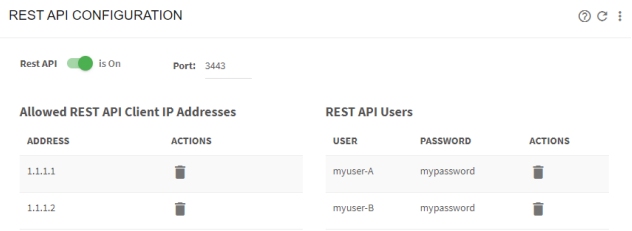
Véase el documento *BQN Guía de Integración con RADIUS* para más detalles.

REST

La API REST API permite integrar el BQN a un sistema externo (ej. un sistema de facturación) para recibir instrucciones de la política que aplicar a cada suscriptor. El API REST se basa en los métodos GET/POST/POST/DELETE de HTTPS con objetos JSON para intercambiar información.

El API REST se pude usar para mapear las políticas definidas localmente en el BQN a una IP de suscriptor y también para definir políticas dinámicas que tomarán precedencia sobre las políticas locales.

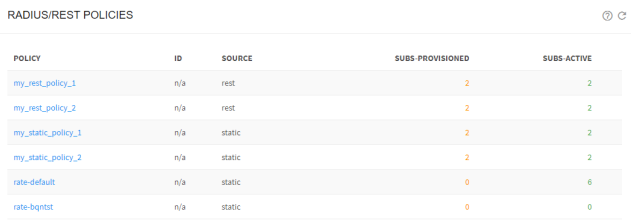
Para configurar el REST API, se va a *Configuration->REST API*. Se añade al menos un usuario/contraseña para autenticar las peticiones REST y se fija el interruptor a On. Opcionalmente, se pueden definir las direcciones IP autorizadas a enviar dichas peticiones.



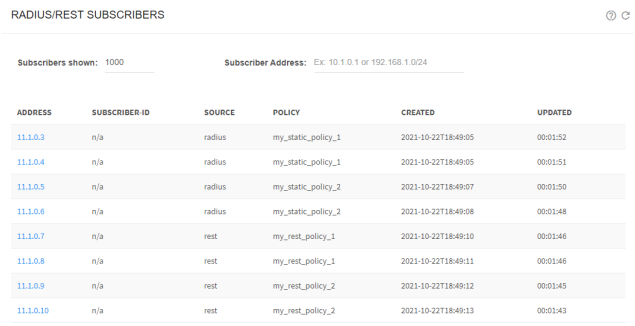
Véase el documento *BQN REST API Guide* para más detalles sobre la definición del API.

Mostrar el estado de API

Para ver la lista de políticas de caudal con su origen (*static* si está definida localmente, REST si se creó vía API REST), seleccione *Status->Radius/REST->Policies*:



Para ver la lista de suscriptores con la política de caudal que ese les está aplicando y su origen (*static* si se asignó por reglas locales, *radius/rest* si se asignó vía API), seleccione to *Status->Radius/REST->Subscribers*:



6.7. Identificación de un Suscriptor

Para el BQN, un tráfico pertenece a un mismo suscriptor si comparte la misma dirección IP en el lado de acceso (en IPv4) o si proviene de la misma subred /64 en el lado de acceso (en IPv6).

Si hubiera un NAT entre el nodo BQN y los clientes reales, los suscriptores cuya dirección IP de acceso se tradujera a una única dirección IP se considerarían como un solo suscriptor.

Un nuevo suscriptor se identifica cuando se recibe su primer paquete de datos IP. En ese momento, se evalúan las reglas tanto de caudal por suscriptor como de monitorización, para elegir qué políticas aplicar en cada caso

6.8. Árbol de Decisión de Flujos por Suscriptor (*Subscriber Flow*)

La evaluación de las reglas de flujos por suscriptores es como sigue: cuando se crea un nuevo flujo de tráfico (por ejemplo, una conexión TCP), se comprueban todos los perfiles del conjunto de reglas de flujo por suscriptor para determinar si el flujo satisface alguno de ellos y establecer así la política de flujo a aplicar.

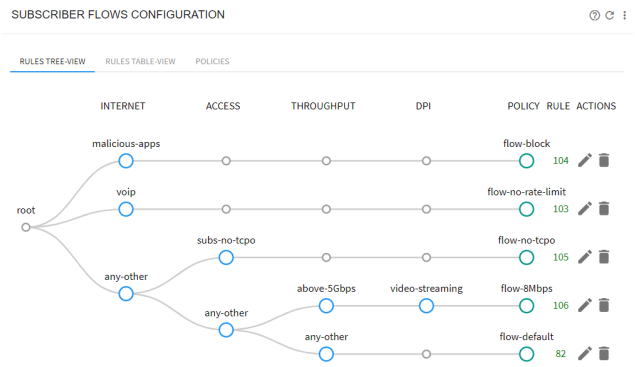
Por eficiencia, los perfiles se evalúan en este orden predefinido:

1. Interfaz (*Interface*)
2. VLAN
3. Internet
4. Acceso (*Access*)
5. DPI
6. Caudal (*Throughput*)

El orden de evaluación de perfiles define un árbol de decisión, cuyos nodos son los diferentes perfiles y con las políticas como hojas. El árbol determina qué regla es finalmente seleccionada, porque una regla puede verse excluida si pertenece a una rama del árbol que no se sigue durante la evaluación. Puede ocurrir que un flujo satisfaga más de una regla. En ese caso, la regla que satisface el perfil de Interfaz tendrá prioridad sobre una que satisfaga un perfil de VLAN, y así sucesivamente, en el orden especificado más arriba.

Si dos reglas satisfacen el mismo tipo de perfil, la de perfil más restrictivo tiene precedencia. Por ejemplo, un flujo de un suscriptor con dirección IP 192.168.0.1 satisface tanto un perfil de acceso con el rango 192.168.0.0/24 y como otro perfil de acceso con el rango 192.168.0.0/16, pero será la primera regla, la asociada al perfil de rango más restrictivo, la seleccionada.

Para facilitar la comprensión de este orden, la GUI incluye una representación gráfica del árbol de decisión, donde el camino coincidente situado más arriba llevará a la política seleccionada (excepto cuando hay más de una política seleccionada en el mismo tipo de perfil, cuando la más restrictiva se impone). Es accesible en *Configuration-> Subscriber Flows*, entrando en la pestaña *RULES TREE-VIEW*.



Si hay elementos comunes en dos perfiles del mismo tipo, y por tanto un conflicto, el árbol de decisión lo señalará para dar la oportunidad al operador de revisar las reglas y corregir el conflicto.

6.9. Árbol de Decisión de Caudal por suscriptor (*Subscriber Rate*)

La evaluación de las reglas de limitación de caudal por suscriptor se realiza cuando se detecta un nuevo suscriptor. Se evalúan los perfiles para determinar los que se cumplen para dicho suscriptor, y de ese modo se determina qué política le corresponde. Por un motivo de eficiencia, los perfiles se evalúan en el siguiente orden predeterminado:

1. Interfaz (*Interface*)
2. VLAN

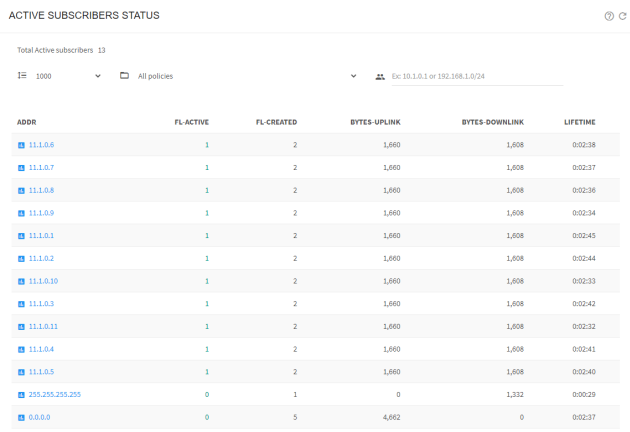
3. Acceso (*Access*)

En las reglas de limitación de caudal por suscriptor, no pueden usarse perfiles del tipo Internet y DPI ya que dichos perfiles no tienen sentido en políticas que se aplican a todo el tráfico de un mismo suscriptor, sea de la aplicación que sea. Tampoco el perfil de caudal, ya que la regla se evalúa al iniciar la sesión y el caudal cambia constantemente.

El árbol de decisión es similar al de flujos por suscriptor. Se accede en *Configuration-> Subscriber Rates*, entrando en la pestaña *RULES TREE-VIEW*.

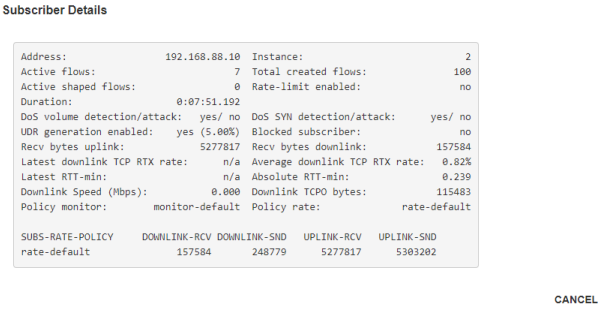
6.10. Comprobar la Política de un Usuario y los Usuarios de una Política

Se puede comprobar qué política se está aplicando a un suscriptor en *Status->Subscribers*. Lista los subscriptores activos, junto con informacion sobre sus flujos y volumen de tráfico:

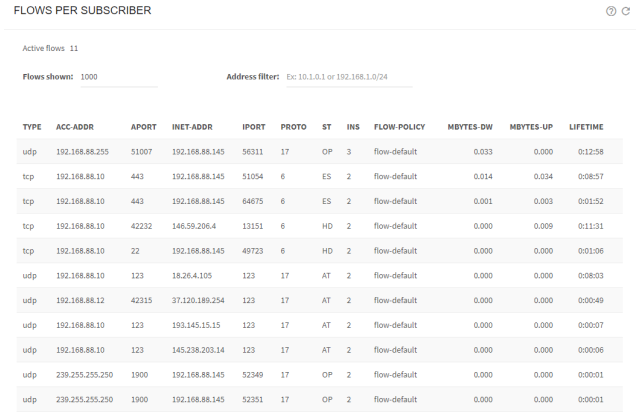


Clicando en el icono justo a la dirección IP, se va a las estadisticas de métricas de ese suscriptor, Clicando en la dirección IP, se proporciona información muy útil como:

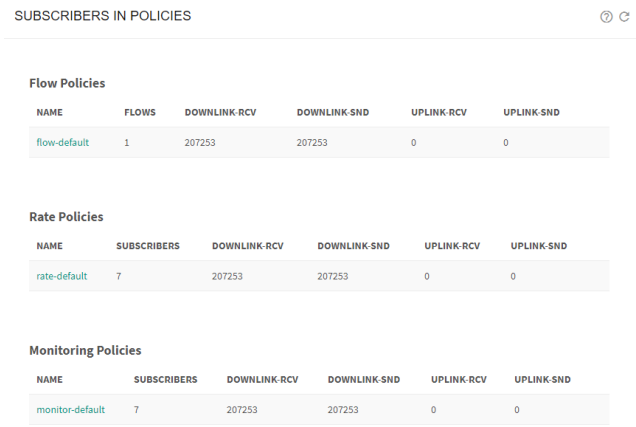
- Política de caudal aplicada (*Policy rate*).
- Política de monitorización aplicada (*Policy monitor*).
- Última medida de retransmisiones en bajada (*Latest downlink TCP RTX rate*) y su valor medio (*Average downlink TCP RTX rate*).
- Última medida en milisegundos de la latencia de acceso mínima (*Latest RTT-min*) y mínimo histórico (*Absolute RTT-min*).



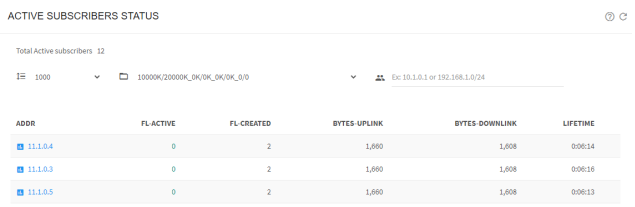
Se puede profundizar en los flujos activos de un suscriptor en *Status->Flows->Per Subscriber*, que muestra la política aplicada a cada flujo, entre otras cosas:



Del mismo modo, se puede ver a cuantos suscriptores se les está aplicando una política dada en *Status->Policies*.



Clicando en una política se listarán los suscriptores actualmente sujetos a dicha política (se mostrarán aquellos con mayor consumo de datos).



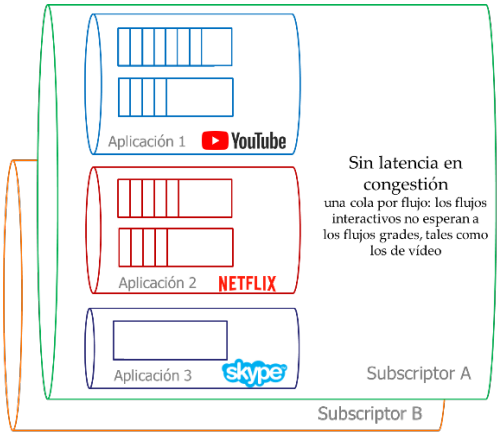
6.11. Ejemplos de Políticas

A continuación, se muestran algunos ejemplos habituales de políticas.

Implementación de Planes de Suscriptores

El objetivo es aplicar los límites de velocidad contratados por cada suscriptor en su plan.

El BQN aplica estos límites mejor que elementos convencionales de shaping porque, para el tráfico TCP (el mayoritario), no necesita descartar paquetes. Más aún, utiliza colas independientes por flujo, lo que independiza las latencias de cada aplicación y mejora enormemente la experiencia de las aplicaciones interactivas. La siguiente imagen muestra la estructura de colas, con una cola por fujo y un control de políticas a nivel de flujos y de suscriptores.



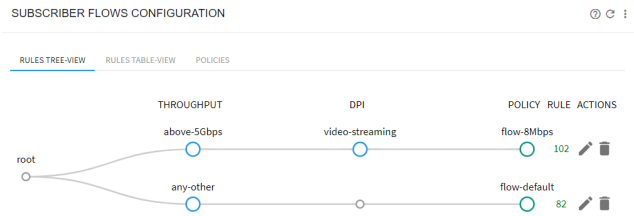
La forma más fácil de implementar planes de suscriptor es configurar el API RADIUS y usar el campo Mikrotik Rate-Limit del RADIUS accounting. Se creará una política dinámicamente con los límites apropiados y se asociará los suscriptores que inician sesión con dicha política. También es possible fijar los límites un poco por debajo de los de los Mikrotik yendo a *Configuration->RADIUS* y cambiando *Mikrotik Rate Limit Scaling* a un valor menos al 100%.

Véase el documento *BQN Guía de Integración con RADIUS* para más detalles.

Límite de Velocidad de Ciertas Aplicaciones

El objetivo es reducir el caudal de red de pico para mitigar la congestión durante la hora cargada. Para ello, se define un perfil de DPI (en este ejemplo, *video*) para identificar las aplicaciones a limitar (ej. *video-streaming*). Este ejemplo utiliza las firmas predefinidas de *streaming*. Para incluirlas, en *Add DPI profile*, seleccionar *Add Predefined Signatures* y elegir la firma predefinida *video-streaming*.

Por otro lado, se crea un perfil de caudal con la carga a partir de la cual aplicar la política (*above-5Gbps* en este ejemplo). Se crea una política de flujos por suscriptor (*flow-8Mbps* en el ejemplo) con un límite de bajada (*Downlink shaping*) fijado a 8 Mbps. Finalmente, el perfil de DPI, el de caudal y la política de flujo se asocian por medio de una regla de políticas de flujo.



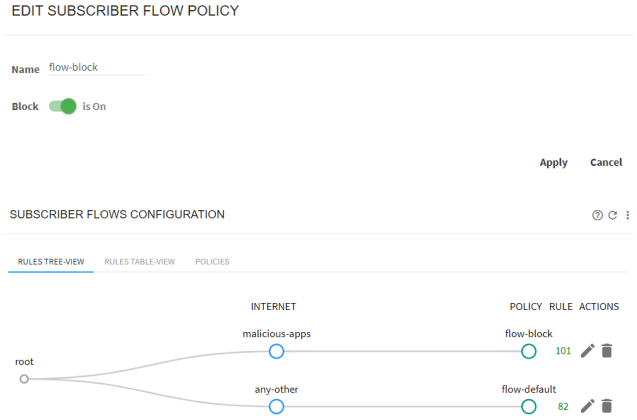
Servicios sin Limitación por el Plan de Suscriptor

El objetivo es preservar la calidad de experiencia de ciertos servicios para que tengan caudal aun cuando el suscriptor usa la totalidad de su caudal, por ejemplo, un servicio de VoIP. Se define un perfil de Internet (*voip*) y una política de flujo (con *Skip subscriber rate limitation* seleccionado). A continuación, se vinculan el perfil de Internet y la política de flujo en una regla de flujo por suscriptor.

Bloqueo de Aplicaciones

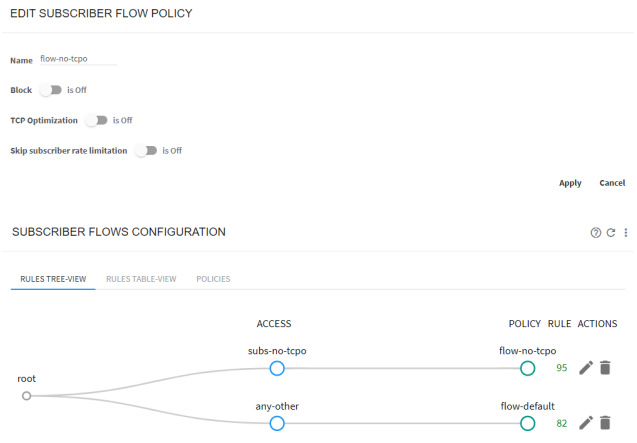
En este escenario, algunas aplicaciones necesitan ser bloqueadas, por ejemplo, servidores que son el

origen de ataques. Para hacerlo, se crea un perfil de Internet (*malicious-apps* en el ejemplo) para identificar las direcciones IP a bloquear. A continuación, se define una política de flujo por suscriptor con una acción de bloqueo (llamado *flow-block* en el ejemplo) y, finalmente se combinan un perfil de Internet y una política de flujo por suscriptor en una regla de flujo.



Excluir Tráfico de la Optimización TCP

El objetivo es que el BQN no optimice cierto tráfico, por ejemplo, ciertos suscriptores. Para ello, se define un perfil de acceso (*subs-no-tcpo* en el ejemplo), con las direcciones IP de los suscriptores a excluir. A continuación, se define una política de flujos por suscriptor con la optimización a off (*flow-no-tcpo* en el ejemplo) y se combinan el perfil de acceso profile y la política de flujos por suscriptor en una regla de flujo.



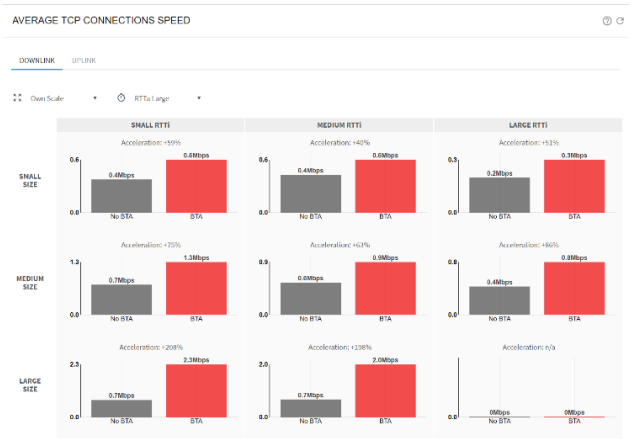
Esta configuración es equivalente a la lista negra de direcciones IP de la Release 3 del BQN.

Otro ejemplo sería usar un perfil de Internet para excluir algunas aplicaciones por su puerto TCP.

7. Métricas de Aceleración TCP

El BQN acelera tráfico TCP para mejorar las velocidades efectivas de transferencia de datos y mejorar la experiencia de los clientes.

En *Status->TCP Acceleration->Speed & Acceleration* se muestran los valores medios de velocidad de una conexión TCP sin aceleración (*no BTA*) y con aceleración (*BTA*). Para tener tráfico comparable, el tráfico se clasifica en nueve categorías en función del tamaño de la descarga y la latencia hasta los servidores de contenido. Los tamaños son: *SMALL SIZE* (hasta 100KB), *MEDIUM* (entre 100KB y 1MB) y *LARGE* (más de 1MB). Las latencias, como distancia (ms) del BQN a los servidores de aplicaciones (*SMALL/MEDIUM/LARGE RTTi*) se definen mediante umbrales configurables que pueden variar de una red a otra. Los valores predefinidos son de menos de 10ms para SMALL RTTi, entre 10ms y 60ms para MEDIUM RTTi y más de 60ms para LARGE RTTi.



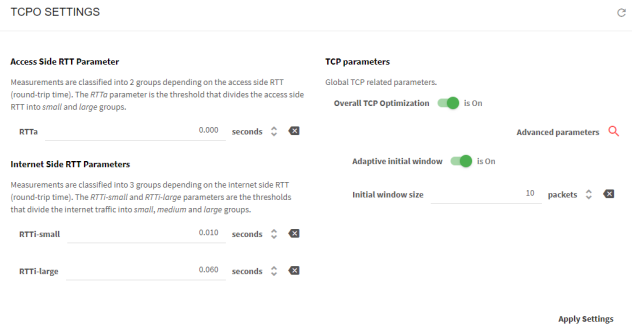
Los valores se muestran para las direcciones de bajada (*downlink*) y subida (*uplink*).

En casos en los que los clientes tengan latencias de acceso muy distintas, pueden clasificarse en dos categorías (*RTTa Small/Large*). El umbral es configurable (ver configuración de los umbrales de latencia al final de esta sección).

Nada más arrancar o tras cambios en los umbrales, las métricas empiezan de cero. El BQN necesitará tiempo para recolectar suficientes métricas antes de poder mostrar resultados. Si no hay suficientes muestras, o la aceleración no es estadísticamente significativa, no mostrará resultados.

En *Statistics->TCP Optimization->TCP Speed* se muestra la evolución temporal de las velocidades:

Para **configurar los umbrales de latencias** usados por las métricas de aceleración, ir a *Configuration->TCPO Settings*.



Permite definir los umbrales para la clasificación por latencia hacia Internet en las métricas de aceleración (*RTTi-small* y *RTTi-large*) y de latencia de acceso (*RTTa*).

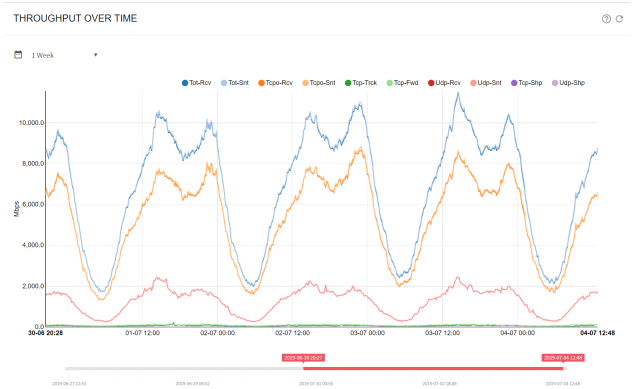
Para deshabilitar totalmente la optimización TCP en el BQN, con independencia de lo que dicten las políticas de flujo, poner el toggle *Overall TCP Optimization* a off. Esto se hace para deshabilitar el TCPO temporalmente mientras se investiga algún problema.

Si hay un NAT entre el BQN y los suscriptores, el toggle *Adaptive Initial Window* debe estar a off.

También es possible modificar la ventana inicial de TCP de 10 paquetes por defecto. Se recomienda únicamente para despliegue con mucha latencia, como un enlace por satélite.

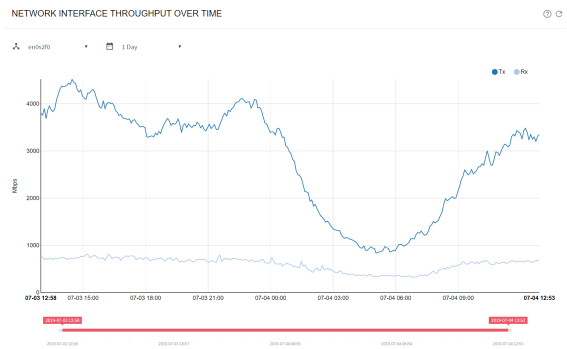
8. Tráfico y Latencias

En *Statistics->Throughput->Overview* se muestra la evolución temporal del caudal de tráfico total, sumando ambas direcciones y todos los *wires*.



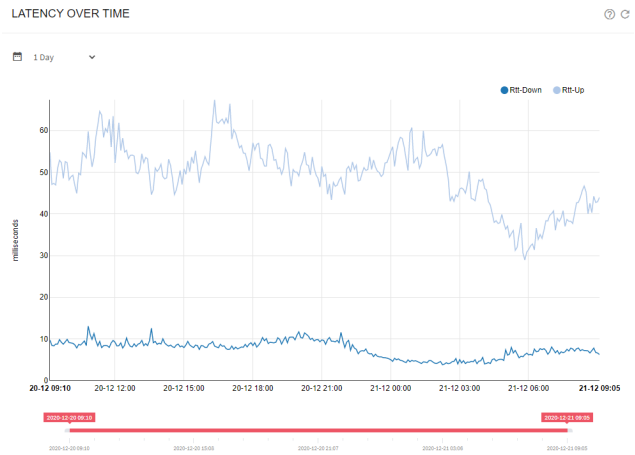
En esta gráfica también se muestra en *Policy* el caudal sujeto a cualquiera de las políticas configuradas.

La evolución temporal por interfaz de red está disponible en *Statistics->Throughput->Interfaces*.



Se puede comprobar qué caudal está siendo procesado conforme a cada una de las distintas políticas configuradas. Para las políticas de flujo por suscriptor, se pueden ver en *Statistics->Throughput->Subscriber Flows Policies* y análogamente para *Subscriber Rate Policies* y *Subscriber Monitoring Policies*.

La gráfica en *Statistics-.>System->Latencies* representa el RTT de acceso (RTT-Down) y el RTT de Internet (RTT-Up) a lo largo del tiempo. Se muestras valores medios para todos los flujos del mínimo por flujo. Pueden servir de referencia para los umbrales de métricas de TCP configurados en *Configuration->General Settings*.



En *Statistics->System->Retransmissions* se muestran los porcentajes medios de retransmisiones en subida y bajada.

También se pueden ver el número de flujos por política y por protocolo *en Statistics->Flow->Per Policy* y *Statistics->Flow->Per Protocol* respectivamente.

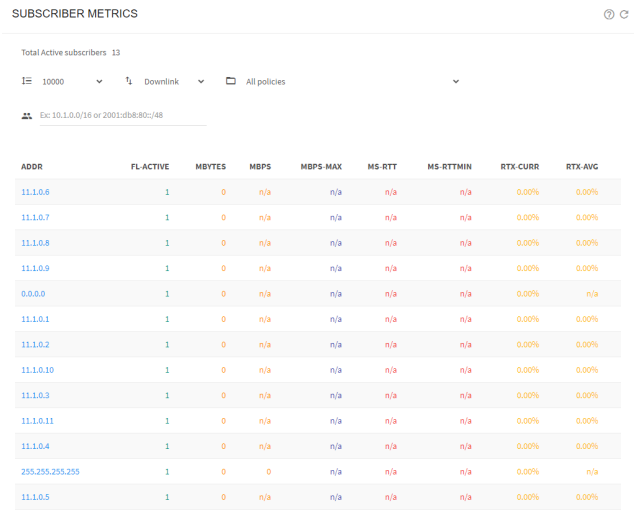
En cada momento, se puede ver el número de flujos activos por protocolo en *Status->Flows->Per Protocol* y por suscriptor en *Status->Flows->Per Subscriber.*

9. Visibilidad (Analíticas)

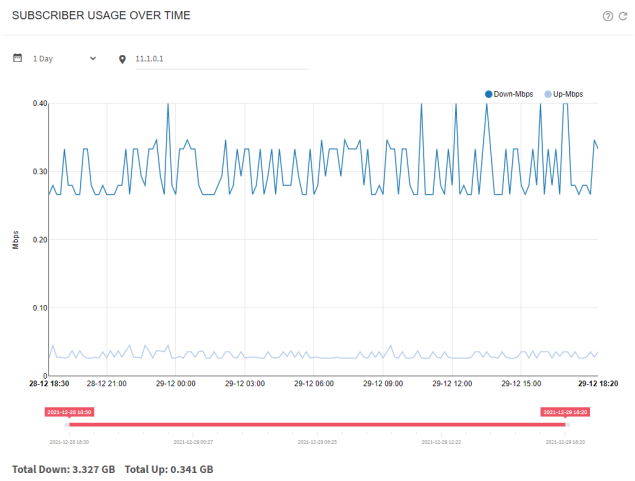
9.1. Métricas por Suscriptor

En *Statistics->Subscribers->Metrics* se obtiene informacion de distintas métricas por suscriptor. Se listan varios suscriptores. Si el deseado no está listado, se pueden obtenerse sus métricas introduciendo su dirección IP en el campo de filtro.

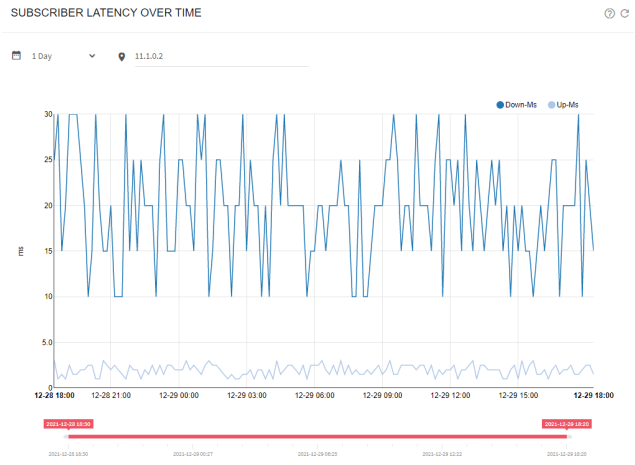
Para cada suscriptor se muestran las métricas más recientes (flujos, caudal, latencias, retransmisiones, etc.).



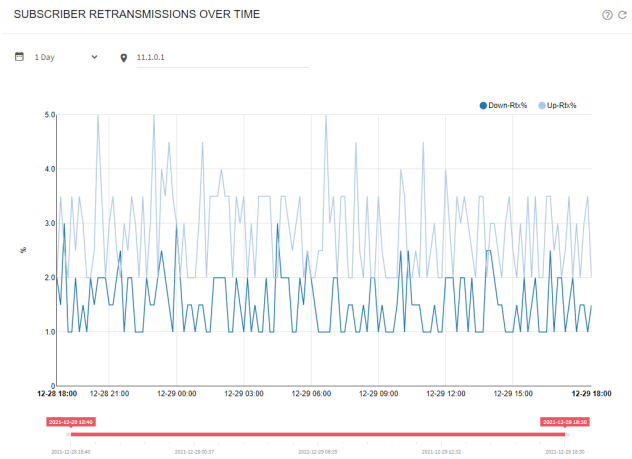
Clicando en el valor de una métrica, se accede a la gráfica con su histórico de hasta tres meses atrás. Por ejemplo, pulsando en MB o Mbps se va a la gráfica de uso de volumen en el tiempo.



Otro ejemplo es la gráfica latencias:



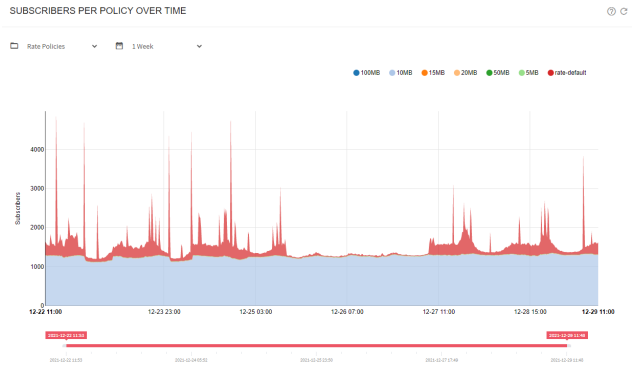
E igualmente de porcentaje de retransmisiones:



Estos valores pueden compararse con los promedios de la red que se muestran en *Statistics->System->Latency* y *Statistics->System->Retransmissions*.

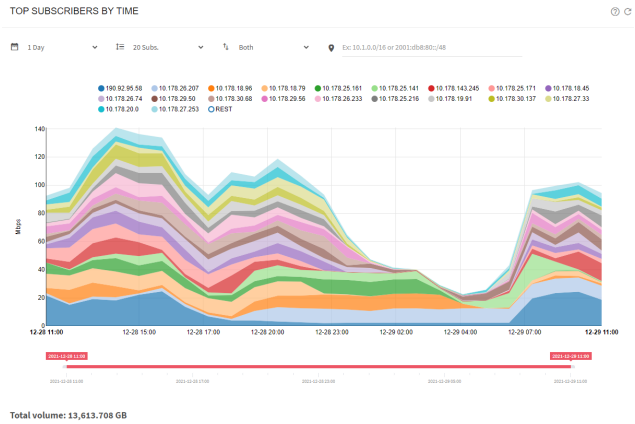
9.2. Tráfico por Política

En *Statistics->Subscribers->Per Policy* se puede ver el reparto del caudal de tráfico entre las distintas políticas de caudal.



9.3. Mayores Consumidores

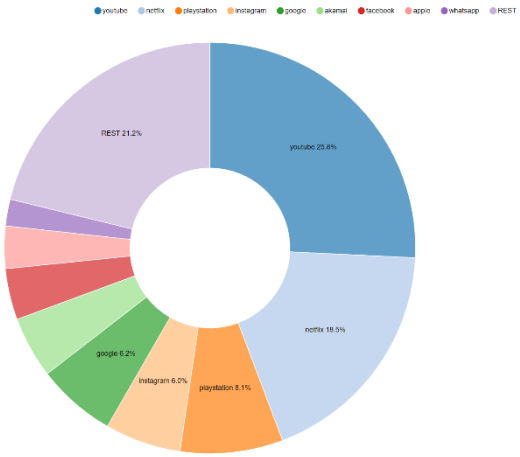
En las opciones *Statistics->Subscribers Analysis->Hourly Volume* y *Statistics->Subscribers Analysis->Total Volume* se muestran las IPs de los clientes con mayores consumos de tráfico a lo largo del tiempo o en el global del periodo considerado, respectivamente.



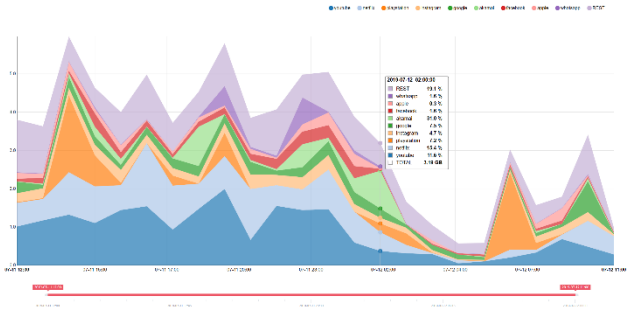
9.4. Tráfico por Servicio

En *Statistics->DPI Analysis* se muestra información sobre la composición del tráfico.

El BQN muestra la composición actual del tráfico por servicio seleccionado *Statistics->DPI Analysis->Total Volume per Service*.



La evolución temporal horaria se obtiene en *Statistics->DPI Analysis->Hourly Volume per Service*.

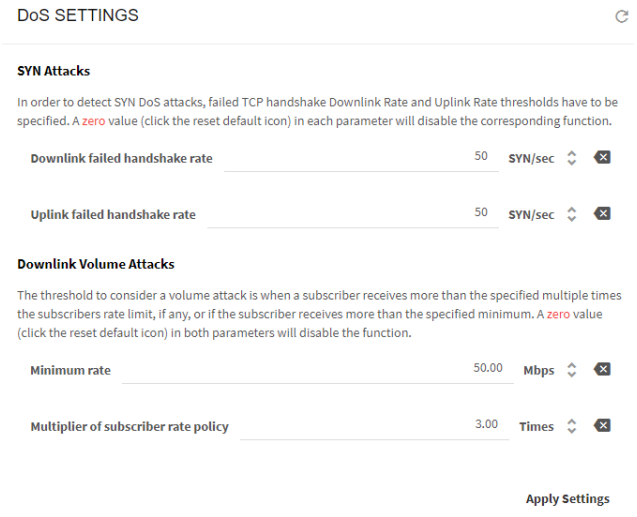


10. DoS

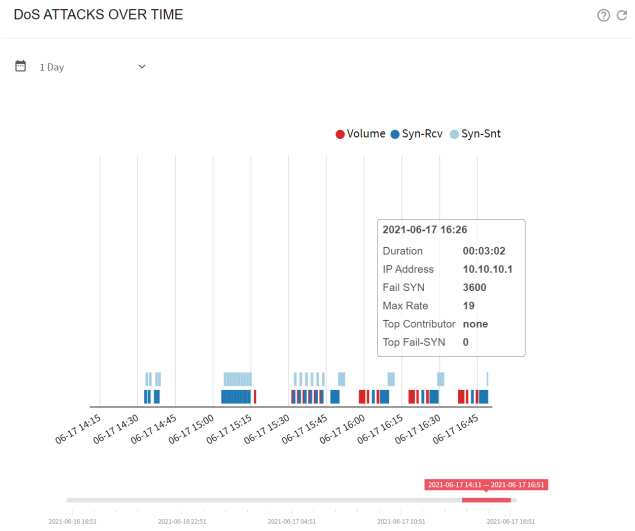
El nodo detecta ataques de denegación de servicio. Para ello hay que definir unos umbrales por encima de los cuales considerar que se está produciendo un

ataque. Dichos umbrales están en Configuration->DoS.

- **Ratio de inicios de conexión fallidos en bajada** (*Downlink failed handshake rate*). Ratio de SYN por segundo en dirección hacia un suscriptor. Un valor típico es 50.
- **Ratio de inicios de conexión fallidos en subida** (*Uplink failed handshake rate*). Ratio de SYN por segundos iniciados por un suscriptor. Un valor típico es 50.
- **Velocidad mínima** (minimum rate). Velocidad mínima que puede ser considerada un ataque. Este valor depende de la velocidad de la red, pero un valor típico es 50Mbps.
- **Multiplicador del límite de política de caudal** por suscriptor (*Multiplier of subscriber rate policy*). Si el suscriptor tiene un plan conocido, se define un umbral como multiplicador*limite de bajada del plan. Un valor típico del multiplicador es 3. Por ejemplo, para un suscriptor de 20Mbps, el umbral sería de 3*20=60Mbps.



Los eventos de DoS se muestran en *Statistics->DoS Attacks*. En *Dos Attacks Over Time* se muestran los distintos ataques con su duración, IP de suscriptor afectada y mayor contribuyente al ataque.



En *SYN Attacks* se listan los ataques de tipo SYN, con el número de SYN fallidos y tasa por segundo. En *Volume Attacks* se detallan los ataques volumétricos, con información del volumen de datos del ataque y su velocidad media.

11. Tareas de Mantenimiento

11.1. Cómo Actualizar la Licencia

El servidor BQN contactará un gestor de licencias de forma automática, para lo cual la interfaz de gestión debe tener conexión de salida a Internet. En caso de que se precise, se puede cargar una licencia localmente en el servidor. La licencia es un fichero con extensión `.lic` proporcionado por Bequant. Se carga seleccionando *Administration->License* y pulsando el icono ⋮ para ir a la opción *Load…* Un selector de fichero permitirá cargar la licencia.

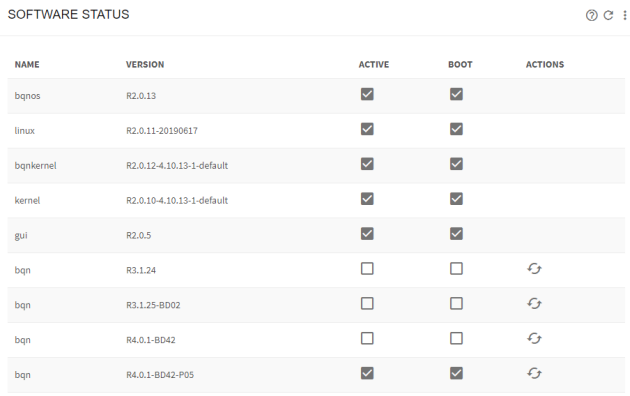
11.2. Cómo Actualizar el Software

La actualización de un paquete bqn-R*.bpkg (ej. bqn-R4.0.1.bpkg) se realiza en dos pasos: primero se instala y posteriormente se activa. La activación supone un corte de tráfico de típicamente diez segundos, por lo que conviene hacerlo en horas de poco tráfico.

La instalación se hace en *Administration->Software* y pulsando el icono ⋮ para seleccionar la opción *Install…* Un selector de fichero permite seleccionar el paquete, que es transferido al servidor e instalado.

La activación se hace en *Administration->Software* pulsando el icono 🔄 en el paquete que se desea activar. Esta operación obliga a hacer login de nuevo

tras algunos segundos durante los cuales hay pérdida de servicio.



11.3. Cómo Generar un Diagnóstico

Cuando lo solicite el soporte de Bequant, se generara un fichero de diagnóstico en *Administration->Diagnostic*.

11.4. Cómo Guardar la Configuración

Se puede guardar la configuración del servidor un fichero local con la opción *Administration->Backup->Save*.

Para restaurar una configuración pasada, seleccione su fichero de backup con la opción *Administration->Backup->Load*.

Se recomienda cargar siempre la configuración sin sobreescritura, de modo que la configuración de interfaces de red no se pierda al transferir una configuración de un servidor BQN a otro.