Application Note
How to use Quality of Service

This application note describes how to use Quality of Service.

The document consists of standard instructions that may not fit your particular solution. Please visit our support website for more information and latest revisions of document and firmware:

http://www.secomea.com/Service-and-Support-85.aspx

Version 1.00, 2010

TrustGate

secomea

Table of Contents

1. Abbreviations and acronyms

QoS	Quality of Service
ISP	Internet Service Provider
DS	DiffServ = Differenced Services
DSCP	Differentiated Services CodePoint
RTP	Real Time Transport Protocol (Internet protocol for transmitting data such audio and video)
RTSP	Real Time Streaming Protocol (standard for controlling streaming data)
ToS	Type of Service
ToS/DS	As shown in appendix D, you can encode DS using a combination of ToS and “Precedence”

2. What is needed to make TrustGate work with QoS

QoS is supported starting with firmware Release 8.0 (build 4342). This document is written for this firmware version.

3. Nice to know before you start

3.1. The Three Priority Classes/Queues

TrustGate uses three Classes/Queues – HIGH (89%), NORMAL (10%) and LOW (1%). High (89%) means that traffic classified in this class is guaranteed 89% of the WAN bandwidth.

At any time, if a higher queue is not using its bandwidth it is possible for a lower queue to borrow from this queue. For example, even if traffic classified as LOW Priority will be able to use the whole bandwidth if no higher class traffic is using it.

3.2. *Queuing disciplin*

The LOW and NORMAL class/queue uses SFQ (Stochastic Fairness Queuing) meaning that all connections will get equal parts of the bandwidth in their class.

The HIGH class/queue uses FIFO (First In First Out). This system has a minimum of delay.

3.3. *Default*

All traffic is classified as NORMAL. In other words, traffic that does not match any rule in the QoS classification table gets placed in the NORMAL queue.

3.4. Stateful Inspection

The QoS engine does not use stateful inspection. This means that if you want to affect both incoming and outgoing traffic, you must create a separate rule for each traffic direction. There are exceptions which are described in this “How to”.

4. The 3 steps

1. Set the Bandwidth on the WAN interface
2. If your applications are using ToS/DS then set the DiffServ Domain Model = Uniform
3. Choose one of the scenarios below.

4.1. Step 1: Set the bandwidth on the WAN interface

To make Quality of Service work you must set the bandwidth of your internet connection:

SYSTEM > WAN > Rx Bandwidth // Tx Bandwidth

It is important that the configured value is below the actual value. For example, meaning if the ISP specifies the internet connection to 1024kbit/sec (download or upload), the value you set in the TrustGate probably should be set 5% lower, like 980kbit/sec.

It is always a good idea to test the actual bandwidth. There are different ways to do this:

A) Perform an FTP download and an FTP upload.

B) There are several services on the Internet which give you tasks for testing your bandwidth.

4.2. Step 2: If your applications use the Type of Service byte:

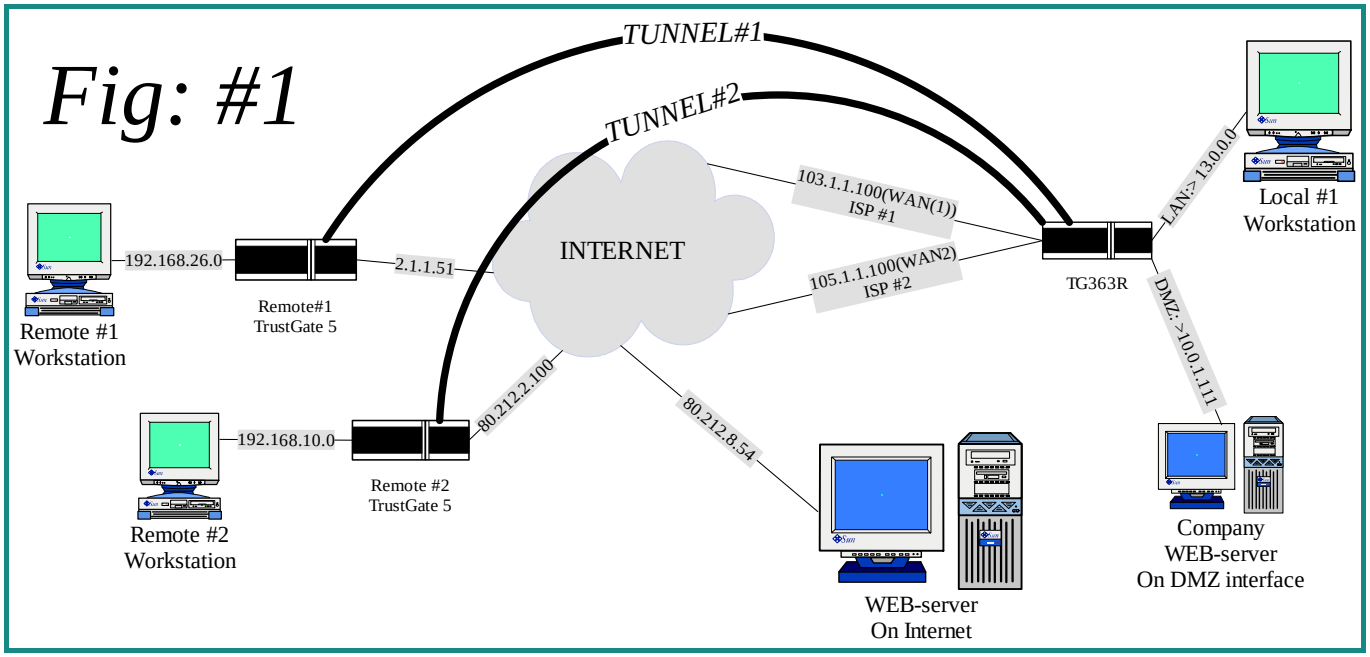
If you are going to use applications that use the ToS byte or DS service and the traffic passes through a tunnel you should set the DiffServ Domain Model = uniform. This will copy the ToS byte to the outer header of the tunnel; this makes it possible to prioritize the tunnel traffic.

VPN > GENERAL > DiffServ Domain Model

4.3. Step 3 Choose a scenario that fits your situation the best

Four scenarios are shown below:

- Prioritize one specific tunnel
- WEB server traffic with highest priority
- Voice over IP using a Software Phone
- Voice over IP using a Hardware Phone (or other phone using the ToS byte)



5. Choose a scenario that fits your situation the best

5.1. Scenario 1) Prioritize one specific tunnel

From Fig: #1 we want to prioritize the traffic from Remote #1.

All other traffic will be placed in the default normal queue.

The QoS Classification Rule looks like this:

Disable	Class	Precedence	TOS	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Comment
☐	High Priority			ESP	2.1.1.51		WAN	Tunnel traffic from Remote TG5#1
☐	High Priority			TCP		192.168.26.0/24	LAN	Traffic going to the Remote #1 network

Explanation:

Rule 1: All encrypted data (protocol ESP) - from the public IP address 2.1.1.51 - incoming on the WAN interface is placed in the HIGH Priority Class/Queue. (*)

Rule 2: All TCP data - to the destination subnet 192.168.26.0 - incoming on the Local LAN interface is placed in the HIGH priority Class/Queue.

*) For more explanation of this scenario, see Appendix B “Dealing with tunneled traffic”.

5.2. Scenario 2) WEB server traffic with highest priority

We want to prioritize the company WEB server on the DMZ interface *(see Fig:#1)*

Disable	Class	Precedence	TOS	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Comment
☐	High Priority			TCP	10.0.1.111 80 http		DMZ	Traffic from an internal WEB server on DMZ interface

Explanation:

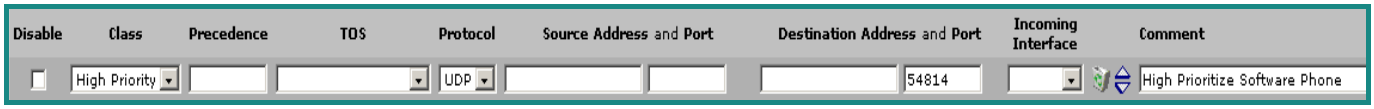
All TCP data - from the WEB server 10.0.1.111 using port 80 (default WEB server port) - incoming on the DMZ interface is placed in the HIGH Priority Class/Queue.

Note: In this case it is only the transmit data that is prioritized. Theoretically we could also prioritize the receive data. However, in web-server use, seen from the browser client, you need bandwidth for downloading, which is transmission from the server. The receive data for the server uses significantly less bandwidth and is therefore placed in the NORMAL Priority Class/Queue.

5.3. Scenario 3) Voice over IP using a Software Phone

In this case we use a software phone like SKYPE (www.skype.com) and force it to use port 54814.

Because both ends are configured to use the same port it is only necessary to configure one rule.



Explanation:

All traffic using the UDP protocol with destination port 54814 is placed in the HIGH priority Class/Queue. (*)

Note: No Incoming Interface is specified because then we would have to make 2 rules. One for incoming WAN with destination port 54814 and one for incoming LAN with Source port 54814. Because the remote client also uses port 54814 the destination port always will be 54814 and there for the above rule can be used for both receiving and transmitting voice data.

Note also that in the above mentioned case we don't expect voice traffic coming from a tunnel but only across the internet.

Note: Some software phones use the ToS byte. If so, configure them the same way as in the scenario with the Hardware phone below.

*) For more explanation of this scenario, see Appendix "Software Phones".

5.4. Scenario 4) Voice over IP using a Hardware Phone (ToS byte)

In most cases a Hardware Phone will use the ToS byte in the traffic pattern for the voice data. When the ToS byte is used, you must remember to set the DiffServ Domain Mode to Uniform (Step 2). But you do not have to think about making pairs of rules.

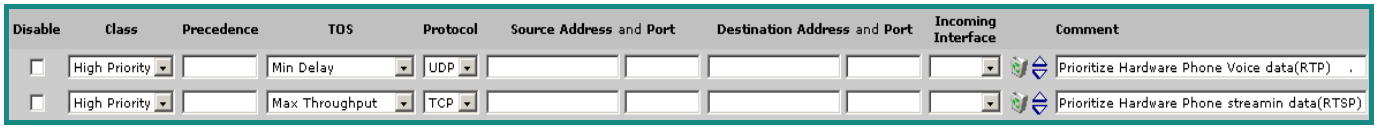
A classification rule could look like this:

Explanation:

All traffic using the ToS byte value "Min Delay" and the Protocol UDP will be placed in the HIGH priority Class/Queue. This rule will both match incoming and outgoing traffic.

Note: In some case other programs might also use the ToS value Min Delay and will there for also match this rule. If so, you should try to narrow the rule even more by specifying a ip address or port.

Additional: If you also want to prioritize the streaming data for the phone conference (RTSP):



Disable	Class	Precedence	TOS	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Comment
☐	High Priority		Min Delay	UDP				Prioritize Hardware Phone Voice data(RTP)
☐	High Priority		Max Throughput	TCP				Prioritize Hardware Phone streamin data(RTSP)

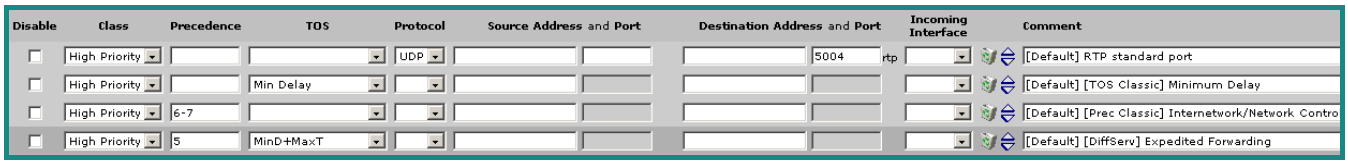
Note: Streaming data is the traffic generated when you call up the remote phone.

Both examples above are compatible with (for example) a Siemens Hardware Phone.

6. Appendix

6.1. A) About the Default rules

The Default rules are shown below. Defaults are only included as examples for using the Classification rules.



Disable	Class	Precedence	TOS	Protocol	Source Address and Port	Destination Address and Port	Incoming Interface	Comment
☐	High Priority			UDP		5004 rtp		[Default] RTP standard port
☐	High Priority		Min Delay					[Default] [TOS Classic] Minimum Delay
☐	High Priority	6-7						[Default] [Prec Classic] Internetwork/Network Contro
☐	High Priority	5	MinD+MaxT					[Default] [DiffServ] Expedited Forwarding

Note that it is possible to specify a range of Precedence.

6.2. B) Dealing with tunneled traffic

The text below is pasted from the TrustGate on-line help file and explains some issues regarding tunnel traffic and QoS.

Tunneled traffic needs special consideration:

Packets that are going to enter a tunnel (be encrypted and encapsulated) is not a problem:

You can classify those packets using the private, or inner, addresses. The classification will be preserved during encapsulation and used to put the resulting ESP packet into the correct class in the WAN interface's transmission queue.

Alas, it is not so simple for packets *arriving* via a tunnel. At the time of arrival at the WAN interface (which is the point where the traffic shaping occurs) the packet is encrypted, so the inner addresses are not available for matching by a rule. Instead, the matching criteria must be a combination of protocol = ESP and the source address of the peer, treating all tunneled traffic equally. Alternatively (or additionally), if you let the peer copy the TOS/DiffServ information from the inner header to the outer header, you will be able to classify the incoming ESP packets by that information. On a TrustGate, this is done by setting VPN > General: DiffServ Domain Model to "Uniform".

Note: Don't be tricked into thinking that you can match incoming ESP packets by selecting "Tunnel" in the "Incoming Interface" field. By the time the classifier regards the packet as coming from the virtual Tunnel interface (which is after decryption), it has already left the reception queue. Selecting Tunnel as the incoming interface can only have an effect on how a packet is treated in the transmission queue if it is going to be forwarded out via the WAN interface again (e.g. if this is an 0/0 tunnel), would such a rule have any effect (namely on how it's treated in the transmission *queue).*

6.3. C) Software Phones

The principles shown here can be used with any software phone program that allows you to specify a port for voice traffic.

About multiple phones:

If your setup uses multiple Skype phones behind the same gateway/router the system must have a different port number for each phone, because the Skype Server on the internet will see all the Skype clients behind the same gateway as having the same public IP-Address. In that case you will have to make a classification rule for each software phone. Or you could soften up the rule. For example, you could just prioritize on the UDP protocol or specify a port range instead of just one port number.

About RTP:

Traffic patterns from software phones are not easy to differentiate from the traffic on the network in general. Voice data uses the UDP protocol, so combining UDP with a specially selected port will give a pretty good match. Most phone applications also support RTP. Real time Transport Protocol is a protocol that runs on top for the UDP Protocol. Unfortunately, we do not yet filter on this protocol, which would give an even better match.

6.4. D) Conversion table ToS and DS

If you are using a Differentiated Services (DS) model instead of the classic ToS/Precedence interpretation, you can use the table below to convert between ToS and DSCP:

TOS\Precedence	0	1	2	3	4	5	6	7
Normal	(BE) 0	8	16	24	32	40	48	56
Max Reliability	1	9	17	25	33	41	49	57
Max Throughput	2	(AF11) 10	(AF21) 18	(AF31) 26	(AF41) 34	42	50	58
MaxT+MaxR	3	11	19	27	35	43	51	59
Min Delay	4	(AF12) 12	(AF22) 20	(AF32) 28	(AF42) 36	44	52	60
MinD+MaxR	5	13	21	29	37	45	53	61
MinD+MaxT	6	(AF13) 14	(AF23) 22	(AF33) 30	(AF43) 38	(EF) 46	54	62
MinD+MaxT+MaxR	7	15	23	31	39	47	55	63

BE: Best Effort

AFxy: Assured Forwarding, Class <x>, Drop Precedence Level <y>

EF: Expedited Forwarding

Example: If the application is specified to use DSCP 46 (Expedited Forwarding), you can match this by specifying Precedence=5 and TOS=MinD+MaxT.

DSCP Differentiated Services CodePoint is 6 bit of the DS (Diffserv) (Mode about DSCP in RFC2474)

6.5. E) AUX (TrustGate5, TrustGate 60 and TrustGate 61)

If the AUX interface is used in separation mode all traffic from and to the AUX network will have low priority.

6.6. F) WAN2 (TrustGate 160, TrustGate260, TrustGate363R or TrustGate 460R)

If we use a that has the capability of using 2 WAN interfaces we have to specify a rule for both interfaces.

In a future release, it will be possible to specify WAN in order to define both WAN interfaces.*

Disable	Class	Precedence	TOS	Protocol	Source Address and Port		Destination Address and Port		Incoming Interface		Comment
☐	Low Priority			TCP	80.212.8.54	80 http			WAN		Traffic from the Internet WEB server
☐	Low Priority			TCP	80.212.8.54	80 http			WAN2		Traffic from the Internet WEB server

Explanation:

The table above show a situation where a WEB server on the internet is prioritized LOW. All TCP data coming from the ip address 80.212.8.54 with source port 80 (WEB server) is placed in the LOW priority Class/Queue.

An additional rule for the WAN2 interface is made in case the WAN (1) falls out.

7. Notices

Publication and copyright

Application Note - How to use Quality of Service, version 1.00, 2010

Trademarks

Disclaimer

Secomea A/S reserves the right to make changes to this publication and to the products described herein without notice. The publication of this document does not represent a commitment on the part of Secomea A/S. Considerable effort has been made to ensure that this publication is free of inaccuracies and omissions but we can not guarantee that there are none.

The following paragraph does not apply to any country or state where such provisions are inconsistent with local law:

SECOMEA A/S PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE

SECOMEA A/S SHALL NOT BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR OTHER DAMAGE ALLEGED IN CONNECTION WITH THE FURNISHING OR USE OF THIS INFORMATION.

Secomea A/S
Denmark

CVR No. DK 31 36 60 38

E-mail: sales@secomea.com
www.secomea.com