funkwerk
enterprise communications

# bintec Workshop

# Quality of Service


Version 0.9

**Purpose**

This document is part of the user's guide to the installation and configuration of bintec gateways running software release 7.1.4 or later. For up-to-the-minute information and instructions concerning the latest software release, you should always read our **Release Notes**, especially when carrying out a software update to a later release level. The latest **Release Notes** can be found at www.funkwerk-ec.com.

**Liability**

While every effort has been made to ensure the accuracy of all information in this manual, Funkwerk Enterprise Communications GmbH cannot assume liability to any party for any loss or damage caused by errors or omissions or by statements of any kind in this document and is only liable within the scope of its terms of sale and delivery.

The information in this manual is subject to change without notice. Additional information, changes and **Release Notes** for bintec gateways can be found at www.funkwerk-ec.com.

As multiprotocol gateways, bintec gateways set up WAN connections in accordance with the system configuration. To prevent unintentional charges accumulating, the operation of the product should be carefully monitored. Funkwerk Enterprise Communications GmbH accepts no liability for loss of data, unintentional connection costs and damages resulting from unsupervised operation of the product.

**Trademarks**

bintec and the bintec logo are registered trademarks of Funkwerk Enterprise Communications GmbH.

Other product names and trademarks mentioned are usually the property of the respective companies and manufacturers.

**Copyright**



**Guidelines and standards**

bintec gateways comply with the following guidelines and standards:

R&TTE Directive 1999/5/EG

CE marking for all EU countries and Switzerland

You will find detailed information in the Declarations of Conformity at www.funkwerk-ec.com.

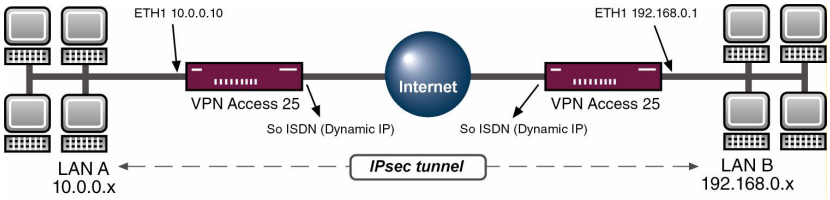
**How to reach Funkwerk Enterprise Communications GmbH**


| | |
|---|---|
| Funkwerk Enterprise Communications GmbH<br>Suedwestpark 94<br>D-90449 Nuremberg<br>Germany<br><br>Telephone: +49 180 300 9191 0<br>Fax: +49 180 300 9193 0<br>Internet: www.funkwerk-ec.com | Bintec France<br>6/8 Avenue de la Grande Lande<br>F-33174 Gradignan<br>France<br><br>Telephone: +33 5 57 35 63 00<br>Fax: +33 5 56 89 14 05<br>Internet: www.bintec.fr |

# 1 Introduction

**The configuration of QoS (Quality of Service) is described below in connection with IPSec. IPSec data are then transferred prioritized. The Setup Tool is used for the configuration.**

## 1.1 Scenario




## 1.2 Requirements

The following are required for the configuration:

- Two Bintec **VPN Access 25** gateways.
- Internet connection at each site.
- IPSec tunnel.
- Your LAN must be connected to the Ethernet interface (ETH 1) of your gateway.
- Your xDSL modem must be connected to the Ethernet interface (ETH 3).
- A configured PC (see User's Guide Part **Access and Configuration**).

**Note**

Use the Bintec **User's Guide** or the Bintec FAQs to configure the Internet connections.

# 2 Configuration of Interfaces

**Explanation:**

The following three protocols are used for an IPSec tunnel.

- Internet Key Exchange (IKE), UDP Port 500.
- Encapsulation Security Payload (ESP).
- Authentication Header (AH).

## 2.1 Configuring an IP Filter for IKE

- Go to ***QoS ➜ IP Filter ➜ ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][FILTER][][ADD]                                              vpn25

  Description                 IPSec (IKE)
  Index

  Protocol  udp

  Source Address
  Source Mask
  Source Port                 specify
  Specify Port                500

  Destination Address
  Destination Mask
  Destination Port            specify
  Specify Port                500
  Type of Service (TOS)       00000000          TOS Mask  00000000

        SAVE                            CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Description | Name of filter. |
| Protocol | The protocol used. |

| Field | Meaning |
|---|---|
| Source Port | The source port used. |
| Specify Port | The port to be used. |
| Destination Port | Destination port to be used. |
| Specify Port | The port to be used. |

Table 2-1: Relevant fields in ***QoS ➜ IP Filter ➜ ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***Description***, e.g. *IPSec (IKE)*.
- Set ***Source Port*** to *specify*.
- Enter *500* as ***Specify Port***.
- Set ***Destination Port*** to *specify*.
- Enter *500* as ***Specify Port***.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

## 2.2 Configuring an IP Filter for ESP

- Go to ***QoS ➜ IP Filter ➜ ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS] [FILTER] [] [ADD]                                          vpn25

  Description                 IPSec (ESP)
  Index

  Protocol  esp

  Source Address
  Source Mask
  Source Port                 any


  Destination Address
  Destination Mask
  Destination Port            any

  Type of Service (TOS)       00000000              TOS Mask  00000000

           SAVE                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Description | Name of filter. |
| Protocol | The protocol used. |

Table 2-2: Relevant fields in ***QoS → IP Filter → ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***Description***, e.g. *IPSec (ESP)*.
- Set ***Protocol*** to *esp*.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

## 2.3 Configuring an IP Filter for AH

- Go to ***QoS*** ➜ ***IP FILTER*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][FILTER][][ADD]                                              vpn25

  Description                 IPSec (AH)
  Index

  Protocol  ah

  Source Address
  Source Mask
  Source Port                 any


  Destination Address
  Destination Mask
  Destination Port            any

  Type of Service (TOS)       00000000              TOS Mask  00000000

            SAVE                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Description | Name of filter. |
| Protocol | The protocol used. |

Table 2-3: Relevant fields in ***QoS*** ➜ ***IP FILTER*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Enter a name under ***DESCRIPTION***, e.g. *IPSec (AH)*.
- Set ***PROTOCOL*** to *ah*.
- Leave all the other settings as they are.
- Press **SAVE** to confirm your settings.

This gives the following filter overview:

- Go to ***QoS → IP FILTER.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][FILTER]: Configure IP Classification Filter                vpn25

  Abbreviations: sa (source IP address)          sp (source port)
                 da (destination IP address)     dp (destination port)
                 it (icmp type)                 estab (TCP established)

  Index Descr           Conditions
  1     IPSec (IKE)     udp, sp 500, dp 500
  2     IPSec (ESP)     esp
  3     IPSec (AH)      ah



     ADD                 DELETE              EXIT
```

Select **EXIT**. You have returned to the ***QoS*** main menu.

# 3 Classification of Data

**The IP Classification and Signaling menu defines how the IPSec packets detected by the IP filters are to be handled.**

Here you define that packets of all three IP filters created are placed in the queue ***CLASS*** *normal* (also called 'class-based') with the ***ID*** *1*.

## 3.1 Classification of IKE Data

- Go to ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALING*** ➜ ***ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][ADD]                                                vpn25

     Filter                    IPSec (IKE) (1)
     Direction                 outgoing

     Action                    classify & set TOS M

     Classification >
     Signaling (TOS) >



        SAVE                                   CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Filter | Filter to be used. |
| Direction | Direction of data traffic. |
| Action | Defines how a filtered data packet is to be handled. |

Table 3-1: Relevant fields in ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALING*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***FILTER*** to *IPSec (IKE)*.
- Set ***DIRECTION*** to *outgoing*.
- Set ***ACTION*** to *classify & set TOS M*.
- Change to the ***CLASSIFICATION*** submenu.

- Go to ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD ➜ CLASSIFICATION.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][ADD][CLASS]: Configure IP QoS Classification        vpn25


    Class Type                    normal
    Class ID                      1


           OK                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Class Type | Defines the class for the IP packets that match the filter conditions. |
| Class ID | The ***CLASS ID*** is used for the class assignment. |

Table 3-2: Relevant fields in ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD ➜ CLASSIFICATION***

Proceed as follows to define the necessary settings:

- Set ***CLASS TYPE*** to *normal*.
- Leave ***CLASS ID*** set to *1*.
- Press **OK** to confirm your settings.

You have returned to ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD***.

- Press **SAVE** to confirm your settings.

## 3.2 Classification of ESP Data

- Go to ***QoS*** ➜ ***IP Classification and Signaling*** ➜ ***ADD***.

**Note**

Make sure the rule chain is correct. The second rule must be placed after the first rule and the third rule after the second.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][ADD]                                                 vpn25

     Filter                    IPSec (ESP) (2)
     Direction                 outgoing

     Action                    classify & set TOS M

     Classification >
     Signaling (TOS) >


     Insert behind Rule        RI 1   FI 1   (IPSec (IKE))


          SAVE                                  CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Filter | Filter to be used. |
| Direction | Direction of data traffic. |
| Action | Defines how a filtered data packet is to be handled. |

Table 3-3: Relevant fields in ***QoS*** ➜ ***IP Classification and Signaling*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***Filter*** to *IPSec (ESP) (2)*.

- Set ***DIRECTION*** to *outgoing*.
- Set ***ACTION*** to *classify & set TOS M*.
- Set ***INSERT BEHIND RULE*** to *RI 1  FI 1  (IPSec (IKE))*.
- Press **SAVE** to confirm your settings.

## 3.3 Classification of AH Data

- Go to ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][CLASS][EDIT]                                                vpn25

     Filter                    IPSec (AH) (3)
     Direction                 outgoing

     Action                    classify & set TOS M

     Classification >
     Signaling (TOS) >


     Next Rule                 RI 2   FI 2   (IPSec (ESP))

          SAVE                                  CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Filter | Filter to be used. |
| Direction | Direction of data traffic. |
| Action | Defines how a filtered data packet is to be handled. |

Table 3-4: Relevant fields in ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD***

Proceed as follows to define the necessary settings:

- Set ***FILTER*** to *IPSec (AH)*.

- Set ***DIRECTION*** to *outgoing*.
- Set ***ACTION*** to *classify & set TOS M*.
- Set ***INSERT BEHIND RULE*** to *RI 2  FI 2  (IPSec (ESP))*.
- Press **SAVE** to confirm your settings.

**Explanation:**

The data detected by the three filters and sent by the gateway is declared as "normal" and placed in the relevant QoS queue.

# 4 Defining QoS Queues and Interfaces

- Go to ***QoS ➜ Interfaces und Policies.***

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT]                                          vpn25

     Interface                              Freenet

     IP QoS Classification via              RI 1   FI 1   (IPSec (IKE))

     QoS Scheduling and Shaping >
     Class-Based QoS Policies >

     MLPPP Interleave Mode                  no

          SAVE                                   CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Interface | The interface to be used. |
| IP QoS Classification via | The filter to be used. |

Table 4-1: Relevant fields in ***QoS ➜ Interfaces und Policies***

Proceed as follows to define the necessary settings:

- Select your WAN partner under ***Interface***, e.g. *Freenet*.
- Select the first rule *RI 1 FI 1 (IPSec (IKE)).*
- Leave ***MLPPP Interleave Mode*** set to *no*.
- Change to ***QoS Scheduling and Shaping***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][SCHEDULER]: Configure QoS Scheduling     vpn25
                                    and Shaping

     Queueing and Scheduling Algorithm  priority queueing (PQ)

     Specify Traffic Shaping            yes

     Maximum Transmit Rate (Bits per Second)      128000


               OK                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Queueing and Scheduling | Activates and deactivates QoS on the interface algorithm. |
| Specify Traffic Shaping | Activates and deactivates bandwidth bounding. |
| Maximum Transmit Rate (Bits per Second) | Indicates the maximum bandwidth of the interface. |

Table 4-2: Relevant fields in ***QoS ➜ Interfaces und Policies***

Proceed as follows to define the necessary settings:

- Set ***Queueing and Scheduling Algorithm*** to *priority queueing (PQ)*.
- Set ***Specify Traffic Shaping*** to *yes*.
- Enter the maximum bandwidth under ***Maximum Transmit Rate (Bits per Second)***, e.g. *128000*.
- Press **OK** to confirm your settings.
- You return to ***QoS ➜ Interfaces und Policies***.

## 4.1 Configuring the Queue and Bandwidth Bounding

The queue configuration and bandwidth bounding are set here. Create an entry for a *class-based* queue. With the ***TRANSMIT RATE*** at *100000* bps, you specify that at least this bandwidth is available for IPSec data packets in overload situations.

- Go to ***QOS*** ➜ ***INTERFACES UND POLICIES*** ➜ ***INTERFACE*** ➜ ***CLASS-BASED QOS POLICIES*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][POLICY][ADD]                              vpn25

     Class                                          class-based
     Class ID                                       1

     Transmit Rate (Bits per Second)                100000



     Weight                                         1
     Priority                                       1

     Shaping Algorithm                              token bucket
     Congestion Avoidance Algorithm                 none
     Dropping Algorithm                             tail drop
     Lower Queue Threshold (Bytes)                  0
     Upper Queue Threshold (Bytes)                  16384

            OK                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Class | Defines the packet class to which this policy is to apply. |
| Class ID | The ***CLASS ID*** is used for the class assignment. |
| Transmit Rate | Defines the bandwidth to be reserved for this class. |

| Field | Meaning |
|---|---|
| Priority | Priority within the “normal” class. The smaller the value, the higher the priority. |

Table 4-3: Relevant fields in ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***Class*** to *class-based*.
- Enter the promised bandwidth under ***Transmit Rate***, e.g. *100000*.
- Set ***Priority*** to *1*.
- Leave all the other settings as they are.
- Press **OK** to confirm your settings.

**Note**

Now create a policy for the remaining traffic. Set ***Class*** to *default*. All packets that do not belong to a queue are processed in this default queue.

- Go to ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***.

```
VPN Access 25 Setup Tool                    Bintec Access Networks GmbH
[QOS][INTERFACES][EDIT][POLICY][ADD]                              vpn25

     Class                                          default

     Transmit Rate (Bits per Second)                0

     Weight                                         1
     Priority                                       255

     Shaping Algorithm                              token bucket
     Congestion Avoidance Algorithm                 none
     Dropping Algorithm                             tail drop
     Lower Queue Threshold (Bytes)                  0
     Upper Queue Threshold (Bytes)                  16384

            OK                                CANCEL
```

The following fields are relevant:

| Field | Meaning |
|---|---|
| Class | Defines the packet class to which this policy is to apply. |
| Priority | Priority within the normal class. The smaller the value, the higher the priority. |

Table 4-4: Relevant fields in ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***

Proceed as follows to define the necessary settings:

- Set ***Class*** to *default*.
- Enter the ***Priority***, e.g. *255*.
- Leave all the other settings as they are.
- Press **OK** to confirm your settings.
- Select **EXIT**.
- Press **SAVE** to confirm your settings.
- You return to ***QoS*** ➜ ***Interfaces und Policies***.

Return to the main menu and finally save your new configuration in the flash memory with ***EXIT*** and ***Save as boot configuration and exit***.

# 5 Prioritization Test

The number of prioritized data packets is shown in the ***QOSPOLICYSTATTABLE***.

Enter the following in the command line of the gateway for this purpose:

```
vpn25:>qosPolicyStatTable
```

```
inx IfIndex(*ro)       Type(ro)             ClassId(ro)
    OutPkts(ro)        OutOctets(ro)        PktsQueued(ro)
    OctetsQueued(ro)   PktsDropped(ro)      OctetsDropped(ro)
    State(rw)

 00 10001              class_based          1
    8                  1356                 0
    0                  0                    0
    running

 01 10001              default              0
    5                  200                  0
    0                  0                    0
    running

vpn25:>qosPolicyStatTable
```

8 prioritized packets with 1356 bytes have been transferred. 5 packets with 200 bytes have been transferred normally.

## 5.1 Overview of Configuration Steps

| Field | Menu | Description | Compulsory field |
|---|---|---|---|
| Description | ***QoS ➜ IP FILTER ➜ ADD*** | e.g. *IKE* | Yes |
| Source Port | ***QoS ➜ IP FILTER ➜ ADD*** | e.g. *specify* | Yes |
| Specify Port | ***QoS ➜ IP FILTER ➜ ADD*** | e.g. *500* | Yes |
| Destination Port | ***QoS ➜ IP FILTER ➜ ADD*** | e.g. *any* | Yes |
| Filter | ***QoS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD*** | *IPSec (IKE) (1)* | Yes |

| Field | Menu | Description | Compulsory field |
|---|---|---|---|
| Direction | **QoS ➜ IP Classification and Signaling ➜ ADD** | *outgoing* | Yes |
| Action | **QoS ➜ IP Classification and Signaling ➜ ADD** | *classify & set TOS M* | Yes |
| Class | **QoS ➜ IP Classification and Signaling ➜ ADD ➜ Classification** | *normal* | Yes |
| Class ID | **QoS ➜ IP Classification and Signaling ➜ ADD ➜ Classification** | *1* | Yes |
| Insert behind Rule | **QoS ➜ IP Classificationand Signaling ➜ ADD** | *RI 1 FI 1(IPSec (IKE))* | Yes |
| Interface | **QoS ➜ Interfaces und Policies** | e.g. *Freenet* | Yes |
| IP QoS Classification via | **QoS ➜ Interfaces und Policies RI 1 FI 1 (IPSec (IKE))** | *Yes* | |
| Queuing and Scheduling Algorithm | **QoS ➜ Interfaces und Policies ➜QoS Scheduling and Shaping** | *priority queueing Yes* | |
| Specify Traffic Shaping | **QoS ➜ Interfaces und Policies ➜QoS Scheduling and Shaping** | *yes* | Yes |
| Maximum Transmit Rate | **QoS ➜ Interfaces und Policies ➜QoS Scheduling and Shaping** | e.g. *128000* | Yes |
| Class | **QoS ➜ Interfaces und Policies ➜ Interface ➜ Class-Based QoS Policies ➜ ADD** | *class-based* | Yes |
| Class ID | **QoS ➜ Interfaces und Policies ➜ Interface ➜ Class-Based QoS Policies ➜ ADD** | *1* | Yes |
| Transmit Rate | **QoS ➜ Interfaces und Policies ➜ Interface ➜ Class-Based QoS Policies ➜ ADD** | e.g. *100000* | Yes |

| Field | Menu | Description | Compulsory field |
|---|---|---|---|
| Priority | ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD*** | e.g. *1* | Yes |
| Class | ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD*** | *default* | Yes |
| Class ID | ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD*** | *255* | Yes |