funkwerk
enterprise communications

bintec Workshop

Quality of Service

Version 0.9

Ziel und Zweck

Dieses Dokument ist Teil des Benutzerhandbuchs zur Installation und Konfiguration von bintec-Gateways ab Software-Release 7.1.4. Für neueste Informationen und Hinweise zum aktuellen Software-Release sollten Sie in jedem Fall zusätzlich unsere **Release Notes** lesen – insbesondere, wenn Sie ein Software-Update zu einem höheren Release-Stand durchführen. Die aktuellsten **Release Notes** sind zu finden unter www.funkwerk-ec.com.

Haftung

Der Inhalt dieses Handbuchs wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Handbuch gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Handbuch können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie **Release Notes** für bintec-Gateways finden Sie unter www.funkwerk-ec.com.

Als Multiprotokollgateways bauen bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

bintec und das bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EG

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Deutschland

Telefon: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

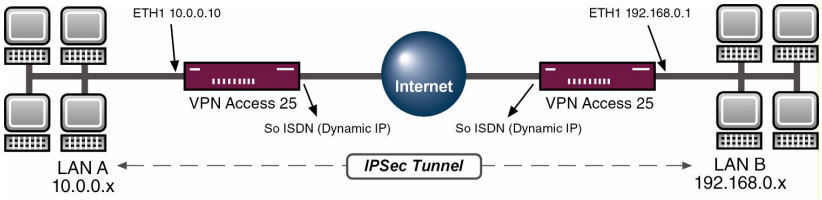
bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
Frankreich

Telefon: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.bintec.fr

1 Einleitung

Im Folgenden wird die Konfiguration von QoS (Quality of Service) in Verbindung mit IPSec beschrieben. Dadurch werden IPSec Daten priorisiert übertragen. Zur Konfiguration wird hierbei das Setup Tool verwendet.

1.1 Szenario



1.2 Voraussetzungen

Folgende Voraussetzungen für die Konfiguration müssen erfüllt sein:

- Zwei Bintec **VPN Access 25** Gateways.
- Internetverbindung an jedem Standort.
- Verfügbarer IPSec-Tunnel.
- Schließen Sie Ihr LAN an die Ethernet-Schnittstelle (ETH 1) Ihres Gateways an.
- Schließen Sie Ihr xDSL-Modem an die Ethernet-Schnittstelle (ETH 3) an.
- PC einrichten, siehe Benutzerhandbuch Teil **Zugang und Konfiguration**.

Hinweis

Zum Einrichten der Internetverbindungen verwenden Sie das Bintec **Benutzerhandbuch** oder die Bintec FAQs.

2 Konfiguration der Interfaces

Erläuterung:

Für einen IPSec-Tunnel werden folgende drei Protokolle verwendet.

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

2.1 Konfigurieren eines IP Filters für IKE

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Name des Filters.
Protocol	Das verwendete Protokoll.

Feld	Bedeutung
Source Port	Quellport.
Specify Port	Der zu verwendende Port.
Destination Port	Zielport.
Specify Port	Der zu verwendende Port.

Tabelle 2-1: Relevante Felder in ***QoS ➜ IP Filter ➜ ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***Description*** einen Namen ein, z.B. *IPSec (IKE)*.
- Wählen Sie unter ***Source Port*** *specify*.
- Tragen Sie als ***Specify Port*** *500* ein.
- Wählen Sie unter ***Destination Port*** *specify*.
- Tragen Sie als ***Specify Port*** *500* ein.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

2.2 Konfigurieren eines IP Filters für ESP

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Name des Filters.
Protocol	Das verwendete Protokoll.

Tabelle 2-2: Relevante Felder in ***QoS ➜ IP Filter ➜ ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***Description*** einen Namen ein, z.B. *IPSec (ESP)*.
- Wählen Sie unter ***Protocol*** *esp*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

2.3 Konfigurieren eines IP Filters für AH

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Description	Name des Filters.
Protocol	Das verwendete Protokoll.

Tabelle 2-3: Relevante Felder in ***QoS*** ➜ ***IP FILTER*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Tragen Sie unter ***DESCRIPTION*** einen Namen ein, z.B. *IPSec (AH)*.
- Wählen Sie unter ***PROTOCOL*** *ah*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Daraus ergibt sich folgende Filterübersicht:

- Gehen Sie zu ***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
```

Wählen Sie **EXIT**. Sie befinden sich wieder im ***QoS*** Hauptmenü.

3 Klassifizierung der Daten

Im Menü IP Classification and Signalling wird definiert, wie mit den durch die IP-Filter erkannten IPSec-Paketen verfahren werden soll.

Hier legen Sie fest, dass Pakete aller drei erstellten IP-Filter in die Queue vom Typ ***CLASS*** *normal* (auch 'Class-Based' genannt) mit der ***ID*** *1* gestellt werden.

3.1 Klassifizierung der IKE Daten

- Gehen Sie zu ***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 >
     Signalling (TOS) >



        SAVE                                  CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Filter	Der zu verwendende Filter.
Direction	Richtung des Datenverkehrs.
Action	Legt fest, wie mit einem gefiltertem Datenpaket verfahren wird.

Tabelle 3-1: Relevante Felder in ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALING*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***FILTER*** *IPSec (IKE)*.
- Wählen Sie unter ***DIRECTION*** *outgoing*.
- Wählen Sie unter ***ACTION*** *classify & set TOS M*.
- Wechseln Sie ins Untermenü ***CLASSIFICATION***.

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Class Type	Definiert den Typ für die IP-Pakete, für welche die Filterbedingungen zutreffen.
Class ID	Durch die ***CLASS ID*** erfolgt die Zuordnung Klasse.

Tabelle 3-2: Relevante Felder in ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD ➜ CLASSIFICATION***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***CLASS TYPE*** *normal*.
- Belassen Sie ***CLASS ID*** bei *1*.

- Bestätigen Sie Ihre Einstellungen mit **OK**.

Sie befinden Sich wieder in ***QoS ➜ IP Classification and Signaling ➜ ADD***.

- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

3.2 Klassifizierung der ESP Daten

- Gehen Sie zu ***QoS ➜ IP Classification and Signaling ➜ ADD***.

Hinweis

Achten Sie auf die Regelverkettung. Die zweite Regel muss hinter der ersten, und die dritte hinter der zweiten Regel plaziert werden.

```
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 >
     Signalling (TOS) >


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


          SAVE                                  CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Filter	Der zu verwendende Filter.
Direction	Richtung des Datenverkehrs.
Action	Legt fest, wie mit einem gefiltertem Datenpaket verfahren wird.

Tabelle 3-3: Relevante Felder in ***QoS ➜ IP Classification and Signaling ➜ ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***FILTER*** *IPSec (ESP) (2)*.
- Wählen Sie unter ***DIRECTION*** *outgoing*.
- Wählen Sie unter ***ACTION*** *classify & set TOS M*.
- Wählen Sie unter ***INSERT BEHIND RULE*** *RI 1 FI 1 (IPSec (IKE))*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

3.3 Klassifizierung der AH Daten

- Gehen Sie zu ***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 >
     Signalling (TOS) >


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

          SAVE                                CANCEL
```

Folgende Felder sind relevant:

Feld	Bedeutung
Filter	Der zu verwendende Filter.
Direction	Richtung des Datenverkehrs.
Action	Legt fest, wie mit einem gefiltertem Datenpaket verfahren wird.

Tabelle 3-4: Relevante Felder in ***QOS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***FILTER*** *IPSec (AH)*.
- Wählen Sie unter ***DIRECTION*** *outgoing*.
- Wählen Sie unter ***ACTION*** *classify & set TOS M*.
- Wählen Sie unter ***INSERT BEHIND RULE*** *RI 2 FI 2 (IPSec (ESP))*.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

Erläuterung:

Die Daten, die durch die drei Filter erkannt und vom Gateway gesendet werden, werden als "normal" deklariert und in die entsprechenden QoS Queue gestellt.

4 Festlegen der QoS Queues und Interfacesfestbelegung

- Gehen Sie zu ***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
```

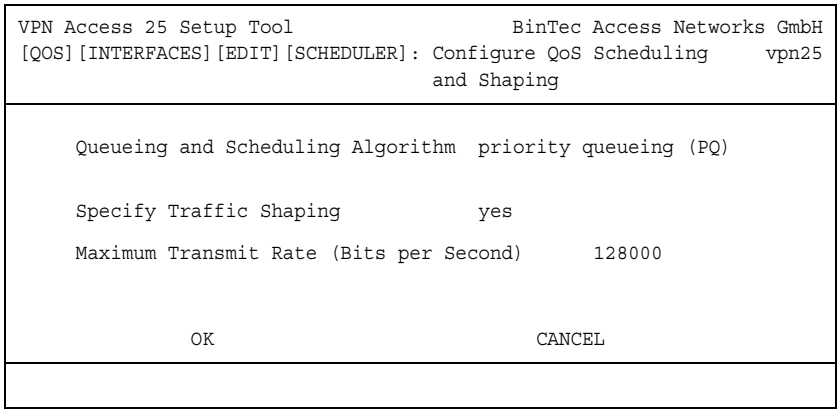
Folgende Felder sind relevant:

Feld	Bedeutung
Interface	Das zu verwendende Interface.
IP QoS Classification via	Das zu verwendende Filter.

Tabelle 4-1: Relevante Felder in ***QoS ➜ Interfaces und Policies***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***Interface*** Ihren WAN Partner, z. B. *Freenet*.
- Wählen Sie die erste Regel *RI 1 FI 1 (IPSec (IKE))*.
- Belassen Sie ***MLPPP Interleave Mode*** bei *no*.
- Wechseln Sie zu ***QoS Scheduling and Shaping***.



Folgende Felder sind relevant:

Feld	Bedeutung
Queueing and Scheduling	Aktiviert bzw. deaktiviert QoS auf dem Interface Algorithm.
Specify Traffic Shaping	Aktiviert bzw. deaktiviert eine Bandbreitenlimitierung.
Maximum Transmit Rate (Bits per Second)	Hier wird die maximale Bandbreite des Interfaces angegeben.

Tabelle 4-2: Relevante Felder in ***QoS ➜ Interfaces und Policies***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***Queueing and Scheduling Algorithm*** *priority queueing (PQ)*.
- Wählen Sie unter ***Specify Traffic Shaping*** *yes*.
- Tragen Sie unter ***Maximum Transmit Rate (Bits per Second)*** die maximale Bandbreite ein, z.B. *128000*.
- Bestätigen Sie Ihre Einstellungen mit **OK**.
- Sie befinden Sich wieder in ***QoS ➜ Interfaces und Policies***.

4.1 Konfigurieren der Queue und Bandbreitenbegrenzung

Hier erfolgt die Queue-Konfiguration und die Bandbreitenbegrenzung. Erstellen Sie einen Eintrag für den Queue *class-based*. Mit ***TRANSMIT RATE*** *100000* Bit/sec legen Sie fest, dass in Überlastungssituationen für IPSec Datenpakete mindestens diese Bandbreite zu Verfügung steht.

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Class	Definiert, für welche Paketklasse die Policy gelten soll.
Class ID	Durch die ***CLASS ID*** erfolgt die Zuordnung der Klasse.
Transmit Rate	Definiert die für diese Klasse zu reservierende Bandbreite.

Feld	Bedeutung
Priority	Priorität innerhalb der "normal"-Klasse. Je kleiner der Wert, desto höher die Priorität.

Tabelle 4-3: Relevante Felder in ***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***Class*** *class-based*.
- Tragen Sie unter ***Transmit Rate*** die zugesicherte Bandbreite ein, z.B. *100000*.
- Wählen Sie unter ***Priority*** *1*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **OK**.

Hinweis

Erstellen Sie nun noch eine Policy für den restlichen Verkehr. Verwenden Sie als ***Class*** *default.* Alle Pakete die nicht einer Queue zugehören, werden in dieser Default-Queue verarbeitet.

- Gehen Sie zu ***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
```

Folgende Felder sind relevant:

Feld	Bedeutung
Class	Definiert, für welche Paketklasse die Policy gelten soll.
Priority	Priorität innerhalb der normal Klasse. Je kleiner der Wert, destso höher die Priorität.

Tabelle 4-4: Relevante Felder in ***QoS ➜ Interfaces und Policies ➜ Interface ➜ Class-Based QoS Policies ➜ ADD***

Gehen Sie folgendermaßen vor, um die notwendigen Einstellungen festzulegen:

- Wählen Sie unter ***Class*** *default*.
- Tragen Sie die ***Priority*** ein, z.B. *255*.
- Belassen Sie alle anderen Einstellungen.
- Bestätigen Sie Ihre Einstellungen mit **OK**.
- Wählen Sie **EXIT**.
- Bestätigen Sie Ihre Einstellungen mit **SAVE**.

- Sie befinden Sich wieder in ***QoS*** ➜ ***INTERFACES UND POLICIES***

Gehen Sie zurück ins Hauptmenü und sichern Sie zum Abschluß Ihre neue Konfiguration im Flashmemory mit ***EXIT*** und ***SAVE AS BOOT CONFIGURATION AND EXIT***.

5 Test der Priorisierung

In der Tabelle ***QOSPOLICYSTATTABLE*** wird die Anzahl der priorisierten Datenpakete angezeigt.

Geben Sie dazu folgendes in die Kommandozeile des Gateways ein:

```
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
```

Es wurden 8 Pakete mit 1356 Bytes priorisiert übertragen. Weiterhin wurden 5 Pakete mit 200 Byte normal übertragen.

5.1 Konfigurationsschritte im Überblick

Feld	Menü	Wert	Pflichtfeld
Description	***QoS ➜ IP FILTER ➜ ADD***	z.B. *IKE*	Ja
Source Port	***QoS ➜ IP FILTER ➜ ADD***	z.B. *specify*	Ja
Specify Port	***QoS ➜ IP FILTER ➜ ADD***	z.B. *500*	Ja
Destination Port	***QoS ➜ IP FILTER ➜ ADD***	z.B. *any*	Ja
Filter	***QoS ➜ IP CLASSIFICATION AND SIGNALING ➜ ADD***	*IPSec (IKE) (1)*	Ja

Feld	Menü	Wert	Pflichtfeld
Direction	***QoS → IP Classification and Signaling → ADD***	*outgoing*	Ja
Action	***QoS → IP Classification and Signaling → ADD***	*classify & set TOS M*	Ja
Class	***QoS → IP Classification and Signaling → ADD → Classification***	*normal*	Ja
Class ID	***QoS → IP Classification and Signaling → ADD → Classification***	*1*	Ja
Insert behind Rule	***QoS → IP Classificationand Signaling → ADD***	*RI 1 FI 1(IPSec (IKE))*	Ja
Interface	***QoS → Interfaces und Policies***	z.B. *Freenet*	Ja
IP QoS Classification via	***QoS → Interfaces und Policies RI 1 FI 1 (IPSec (IKE))***	*Ja*	
Queueing and Scheduling Algorithm	***QoS → Interfaces und Policies →QoS Scheduling and Shaping***	*priority queueing Ja*	
Specify Traffic Shaping	***QoS → Interfaces und Policies →QoS Scheduling and Shaping***	*yes*	Ja
Maximum Transmit Rate	***QoS → Interfaces und Policies →QoS Scheduling and Shaping***	z.B. *128000*	Ja
Class	***QoS → Interfaces und Policies → Interface → Class-Based QoS Policies → ADD***	*class-based*	Ja
Class ID	***QoS → Interfaces und Policies → Interface → Class-Based QoS Policies → ADD***	*1*	Ja
Transmit Rate	***QoS → Interfaces und Policies → Interface → Class-Based QoS Policies → ADD***	z.B. *100000*	Ja
Priority	***QoS → Interfaces und Policies → Interface → Class-Based QoS Policies → ADD***	z.B.*1*	Ja

Feld	Menü	Wert	Pflichtfeld
Class	***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***	*default*	Ja
Class ID	***QoS*** ➜ ***Interfaces und Policies*** ➜ ***Interface*** ➜ ***Class-Based QoS Policies*** ➜ ***ADD***	*255*	Ja