

QUALITY OF SERVICE

Copyright © 24. Juni 2005 Funkwerk Enterprise Communications GmbH
Bintec Workshop
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 Alle Rechte sind vorbehalten. Kein Teil dieses Handbuchs darf ohne schriftliche Genehmigung der Firma Funkwerk Enterprise Communications GmbH in irgendeiner Form reproduziert oder weiterverwertet werden. Auch eine Bearbeitung, insbesondere eine Übersetzung der Dokumentation, ist ohne Genehmigung der Firma Funkwerk Enterprise Communications GmbH nicht gestattet.

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



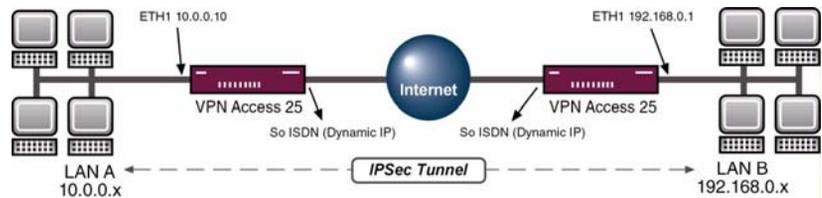
| | | |
|----------|--|-----------|
| 1 | Einleitung | 3 |
| 1.1 | Szenario | 3 |
| 1.2 | Voraussetzungen | 3 |
| 2 | Konfiguration der Interfaces | 5 |
| 2.1 | Konfigurieren eines IP Filters für IKE | 5 |
| 2.2 | Konfigurieren eines IP Filters für ESP | 6 |
| 2.3 | Konfigurieren eines IP Filters für AH | 8 |
| 3 | Klassifizierung der Daten | 11 |
| 3.1 | Klassifizierung der IKE Daten | 11 |
| 3.2 | Klassifizierung der ESP Daten | 13 |
| 3.3 | Klassifizierung der AH Daten | 14 |
| 4 | Festlegen der QoS Queues und Interfacesfestbelegung | 17 |
| 4.1 | Konfigurieren der Queue und Bandbreitenbegrenzung | 19 |
| 5 | Test der Priorisierung | 23 |
| 5.1 | Konfigurationsschritte im Überblick | 23 |



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.



Zum Einrichten der Internetverbindungen verwenden Sie das Handbuch 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 platziert werden.

| | |
|---|--------------------------------------|
| VPN Access 25 Setup Tool [QoS] [CLASS] [ADD] | BinTec Access Networks GmbH vpn25 |
| Filter Direction | IPSec (ESP) (2) 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 [QOS] [CLASS] [EDIT] | BinTec Access Networks GmbH 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 | Der zu verwendende Interface.. |
| IP QoS Classification via | Der 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**.

| | |
|---|-----------------------------|
| VPN Access 25 Setup Tool | BinTec Access Networks GmbH |
| [QOS] [INTERFACES] [EDIT] [SCHEDULER]: Configure QoS Scheduling and Shaping | vpn25 |
| Queueing and Scheduling Algorithm | priority queueing (PQ) |
| Specify Traffic Shaping | yes |
| Maximum Transmit Rate (Bits per Second) | 128000 |
| OK | CANCEL |

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 POLICIE** → **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 POLICIE → 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 POLICIE → ADD**.

| | |
|--|--------------------------------------|
| VPN Access 25 Setup Tool [QOS] [INTERFACES] [EDIT] [POLICY] [ADD] | BinTec Access Networks GmbH 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, desto höher die Priorität. |

Tabelle 4-4: Relevante Felder in **QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → 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. <i>IKE</i> | Ja |
| Source Port | QoS → IP FILTER → ADD | z.B. <i>specify</i> | Ja |
| Specify Port | QoS → IP FILTER → ADD | z.B. <i>500</i> | Ja |
| Destination Port | QoS → IP FILTER → ADD | z.B. <i>any</i> | Ja |
| Filter | QoS → IP CLASSIFICATION AND SIGNALING → ADD | <i>IPSec (IKE) (1)</i> | Ja |

| Feld | Menü | Wert | Pflichtfeld |
|-----------------------------------|--|---------------------------------|-------------|
| Direction | QoS → IP CLASSIFICATION AND SIGNALING → ADD | <i>outgoing</i> | Ja |
| Action | QoS → IP CLASSIFICATION AND SIGNALING → ADD | <i>classify & set TOS M</i> | Ja |
| Class | QoS → IP CLASSIFICATION AND SIGNALING → ADD → CLASSIFICATION | <i>normal</i> | Ja |
| Class ID | QoS → IP CLASSIFICATION AND SIGNALING → ADD → CLASSIFICATION | <i>1</i> | Ja |
| Insert behind Rule | QoS → IP CLASSIFICATION AND SIGNALING → ADD | <i>RI 1 FI 1 (IPSec (IKE))</i> | Ja |
| Interface | QoS → INTERFACES UND POLICIES | <i>z.B. Freenet</i> | Ja |
| IP QoS Classification via | QoS → INTERFACES UND POLICIES RI 1 FI 1 (IPSec (IKE)) | <i>Ja</i> | |
| Queueing and Scheduling Algorithm | QoS → INTERFACES UND POLICIES → QoS SCHEDULING AND SHAPING | <i>priority queueing Ja</i> | |
| Specify Traffic Shaping | QoS → INTERFACES UND POLICIES → QoS SCHEDULING AND SHAPING | <i>yes</i> | Ja |
| Maximum Transmit Rate | QoS → INTERFACES UND POLICIES → QoS SCHEDULING AND SHAPING | <i>z.B. 128000</i> | Ja |
| Class | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | <i>class-based</i> | Ja |
| Class ID | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | <i>1</i> | Ja |
| Transmit Rate | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | <i>z.B. 100000</i> | Ja |
| Priority | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | <i>z.B. 1</i> | Ja |

| Feld | Menü | Wert | Pflichtfeld |
|----------|--|----------------|-------------|
| Class | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | <i>default</i> | Ja |
| Class ID | QoS → INTERFACES UND POLICIES → INTERFACE → CLASS-BASED QoS POLICIE → ADD | 255 | Ja |

