Chapter 29

Managing Services with Enterprise Manager Portal

This chapter describes how IT managers and service providers can use Enterprise Manager Portal to manage subscribers, services, and subscriptions in their enterprises. The chapter contains the following sections:

Overview of Enterprise Manager Portal

IT managers who connect to the SRC network through a JUNOS routing platform or JUNOSe router can use Enterprise Manager Portal to activate services, subscribers, and subscriptions for that enterprise. The services that IT managers can use depend on those that the service provider offers (see *Chapter 27, Installing and Configuring Enterprise Service Portals*). In SRC-managed environments that include both JUNOS routing platforms and JUNOSe routers, the router type determines which types of services can be configured on a system. The portal does not indicate whether a router is a JUNOS routing platform or a JUNOSe router. Table 41 lists the types of services that can be configured from Enterprise Manager Portal for JUNOSe routers and JUNOS routing platforms.

Table 41: Portal Configuration Support for Services on Routers

Type of Service	JUNOSe Router	JUNOS Routing Platform
BoD services	Yes	Yes
VPNs	No	Yes
Applications	No	Yes
Firewall services	No	Yes
NAT services	No	Yes

If you offer Network Address Translation (NAT) services, IT managers can also use the portal to request public IP addresses for use with NAT services on an access.

Getting Help on Enterprise Manager Portal

Most fields in the portal offer tool tips. To view tool tips for a field in the portal, hold the cursor over that field in the portal.

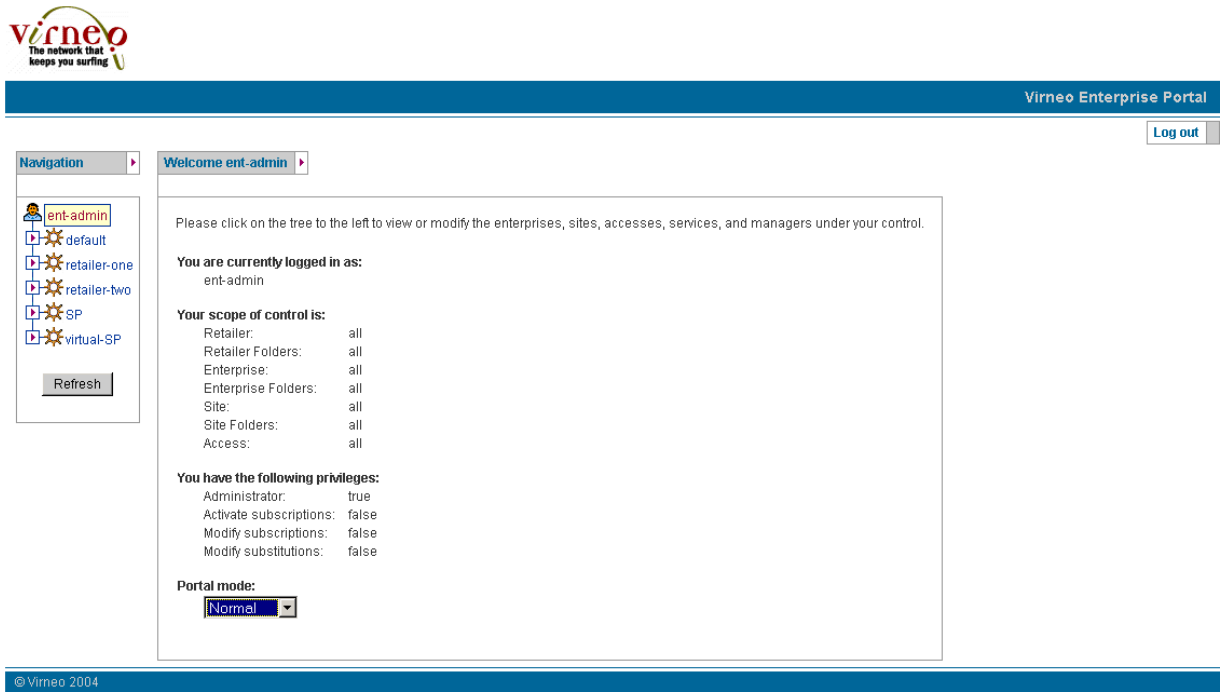
Some fields and pages in the portal offer more extensive online help. To view this help, click the help icon .

Setting the Configuration Level for Enterprise Manager Portal

The default setting for the configuration level is Normal. With this setting you can configure most services on a JUNOS routing platform. If you want to configure more advanced features, such as static source NAT rules, you must change the configuration level of the portal. To do so:

1. Click the operator icon in the navigation pane.

   The operator's Welcome page appears.



2. Select **Advanced** from the Portal mode drop-down list.

Managing Schedules

An IT manager can configure schedules to be applied to BoD or firewall services for a specified enterprise subscriber. From Enterprise Manager Portal, you can establish schedules that identify the times when a specified BoD or firewall service can be activated or deactivated. Schedules are configured on a per-subscriber basis; they cannot be shared with other subscribers. Schedules are, however, inherited by subscribers subordinate to the subscriber for which the schedule is configured.

NOTE: NAT services cannot be scheduled.

Whether or not scheduling is available depends on the configuration for Enterprise Manager Portal and for the service.

To enable scheduling:

1. Edit the *web.xml* file for the portal to enable scheduling. See *Chapter 27, Installing and Configuring Enterprise Service Portals*.

   When scheduling is enabled for the portal, a Schedules tab appears on Enterprise Manager Portal page.

2. Enable scheduling for the BoD or firewall service to be scheduled from Enterprise Manager Portal. See *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

If you plan to schedule BoD or firewall service subscriptions, you can configure the schedules first so that you can assign schedules at the time that you configure the subscription. If the subscriptions are already configured, you can edit the service definition to assign a schedule. The Schedules page lets you create new schedule definitions and view and change existing ones.

Each subscription, whether to the same service or to another one, can have its own schedule.

To use a schedule:

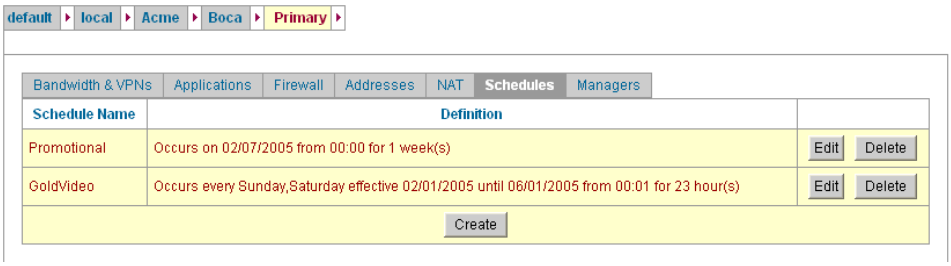
1. Create the schedule. See *Creating a Schedule* on page 468.
2. Apply the schedule to a subscription. See *Applying a Schedule to a Service* on page 472.

Creating a Schedule

To create a schedule:

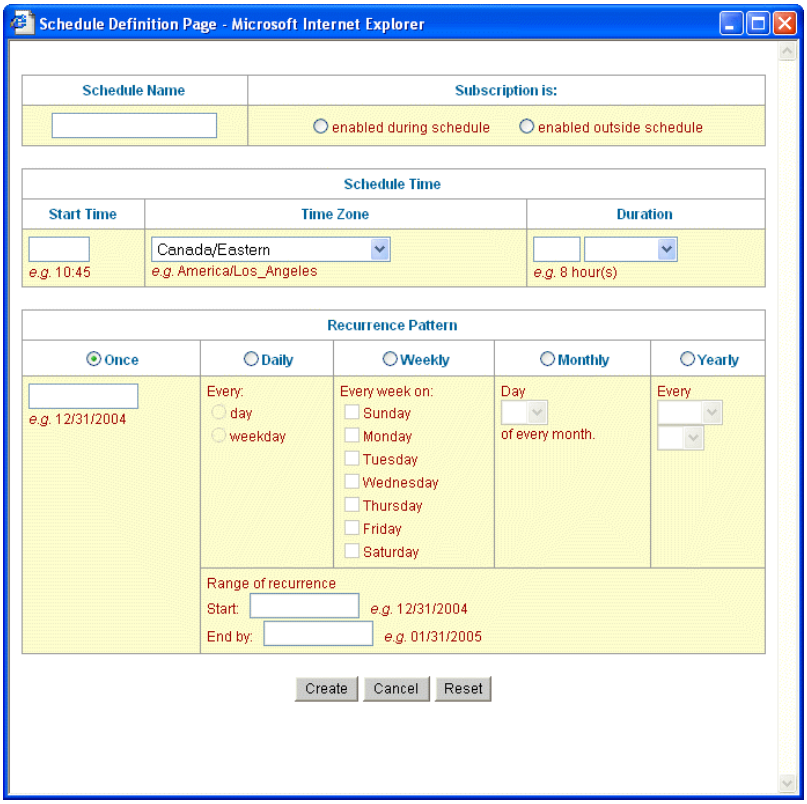
1. Click the **Schedules** tab.

   The Schedules page appears.



2. In the Schedules page, click **Create**.

The Schedule Definition Page appears.



3. Using the field descriptions below, define a schedule, and click **Save**.

   A description of the schedule appears in the Schedules page.

NOTE: The system generates the description of the service. If you want a page to display a different description, you can edit the JSP page and change and compile the Java classes found in the WAR file.

If you need assistance to make these changes, contact Juniper Professional Services.

Schedule Name

- Name of the schedule.
- Value—Text string
- Default—No value

Subscription is

- Whether or not the subscription can be activated during or outside the scheduled time.
- Value
  - Enabled during schedule—Service can be activated during the scheduled time.
  - Enabled outside schedule—Service can be activated outside the scheduled time.
- Default—No value

Start Time

- Time that a scheduled activity is to start.
- Value—Time of day in the format hh:mm, where hh indicates the hour and mm indicates the minute. The range is 00:00 to 23:59.
- Default—No value
- Example—13:15

Time Zone

- Time zone for which the schedule is defined.
- Value—Name of time zone
- Default—Local time zone

Duration

- Length of time after the start time that a scheduled activity is allowed.
- Value—Length of time in minutes, hours, days, or weeks
- Guidelines—The length of time should be more than 15 minutes; using a shorter time could adversely affect system performance. Table 42 shows the maximum duration for specified recurrence patterns.

Table 42: Maximum Duration for Recurrence Patterns

For This Recurrence Pattern	Duration Must Be Less Than
Daily	24 hours
Weekly	24 hours
Monthly	28th day of the month
Yearly	365 days

- Default—No value
- Example—2 hours

  During the interval from the start time to 2 hours after the start time, the action (defined on the Schedule Definition Page under the *During schedule subscription is* field) is available.

Once

- Date on which the scheduled activity is to occur.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value
- Example—12/10/2005

Daily

- Whether or not the scheduled activity is to occur every day of the week or every weekday.
- Value
  - day—Scheduled activity is to occur on every day of the week
  - weekday—Scheduled activity is to occur on each day Monday through Friday
- Default—No value

Weekly

- Scheduled activity occurs on a specified day or days during a week.
- Value—Name of day(s) of the week
- Default—No value

Monthly

- Scheduled activity occurs on the indicated day every month
- Value—Day of the month
- Default—No value

Yearly

- Scheduled activity occurs on a specified day each year
- Value—Month and day
- Default—No value

Range of recurrence Start by

- Date on which a schedule starts for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

  The default indicates that the recurring schedule starts immediately—the next time the recurrence pattern applies.

- Example—12/10/2005

Range of recurrence End by

- Date on which a schedule ends for a recurring action.
- Value—Date in the format mm/dd/yyyy, where mm indicates the month, dd indicates the day, and yyyy indicates the year
- Default—No value

  The default indicates that the schedule has no end date and remains in place indefinitely.

- Example—12/10/2005

Applying a Schedule to a Service

Before you can schedule a subscription, you must define a schedule. See *Creating a Schedule* on page 468.

To apply a schedule to a service that was configured earlier:

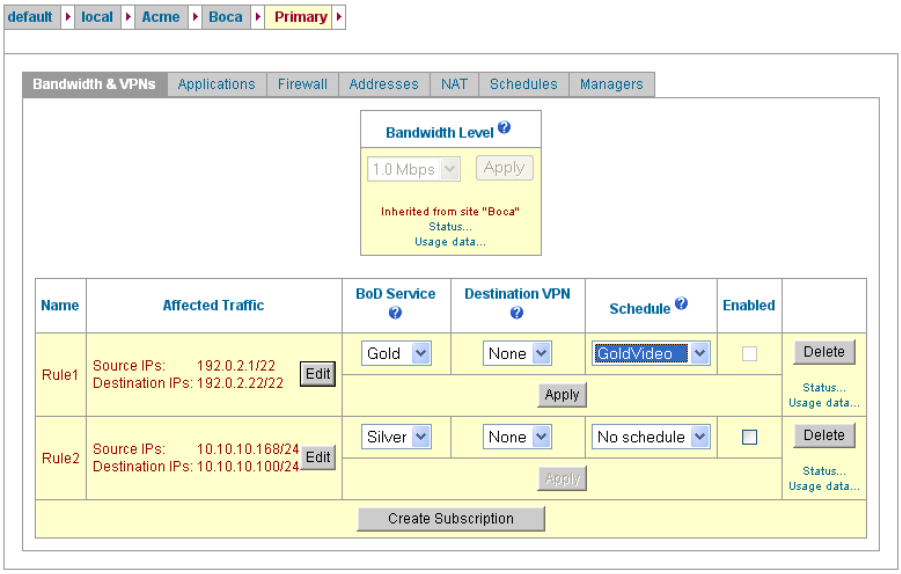
1. In the navigation pane of Enterprise Manager Portal, click the subscriber for which you want to schedule a service.
2. Click the tab for the type of service to be scheduled:
   - Bandwidth or Bandwidth & VPNs
   - Firewall

   NOTE: If VPN features are not configured, the tab is named Bandwidth.

3. On the same line as the service to be assigned to a schedule, select the name of a schedule under Schedule, and click **Apply**.

The service provider controls which services can be scheduled. Text on the page indicates which services cannot be scheduled.



Disabling a Schedule for a Service

When you disable a schedule for a subscription, the service remains in the same state as when the schedule was disabled. For example, if the service is inactive at the time the schedule is removed, the service remains inactive. This state can be different from the one indicated by the Enabled check box. After disabling a schedule for a service, ensure that the status of the service is the same as indicated by the Enabled check box.

To disable a schedule for a service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to remove a schedule that is assigned to a service, and then click the **Bandwidth & VPNs** (or **Bandwidth**) or **Firewall** tab.

2. On the line for the service select **No Schedule**, and then in the last column click the **Status** link.

3. On the Subscription Status page, check the status of the sessions listed. If a session status is different from what it should be—for example if it is inactive instead of active—click **Fix Problems** to activate or deactivate the session.

   See *Monitoring the Status of Subscriptions* on page 520.

Changing Schedules

You can change a schedule at any time. Before you delete a service schedule, however, you must make sure that the schedule is not being used by any service.

To modify a schedule:

1. Click the **Schedules** tab; then on the line that describes the schedule that you want to change, click **Edit**.

2. On the Schedule Edit page, change values using the field descriptions under *Creating a Schedule* on page 468, and click **Apply**.

To delete a schedule:

1. Before you delete a schedule, make sure that none of the services reference this schedule:

   - Go to the Bandwidth (or Bandwidth & VPNs) page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.

   - Go to the Firewall page and review the names of schedules listed under Schedule. If the name of the service to be changed is listed, change the schedule to another one or to Any.

2. Click the **Schedules** tab; then on the line that describes the schedule that you want to delete, click **Delete**.

   The Schedules page no longer lists the schedule.

Managing Subscriptions to Bandwidth-on-Demand Services

The service provider makes bandwidth services available to enterprises. IT managers can use these services to provision bandwidth within an enterprise to meet the forwarding requirements for subscriber traffic. The service provider can make the following types of bandwidth services available:

- Bandwidth-level allocation for an Internet access link

  Only one subscription to one bandwidth level is supported for an access link.

- BoD services that classify traffic and assign different classes of traffic to different BoD services

  You can classify traffic by source IP address, destination IP address, source Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port, destination TCP or UDP port, or type-of-service (ToS) byte, and assign that traffic to a service level.

NOTE: Enterprise Manager Portal supports only services that have policies configured.

When both of these services are available, you can provide subscribers with class of service (CoS)—the method of classifying traffic on a packet-by-packet basis with information in the ToS byte to provide different service levels to different traffic.

Whether bandwidth level (a basic BoD service), BoD services, or both are available depends on the configuration for the portal. See *Chapter 27, Installing and Configuring Enterprise Service Portals*.

Planning Subscriptions to BoD Services

When planning subscriptions, consider the following factors:

- In a configuration that includes both a subscription to a bandwidth level and subscriptions to BoD services, the bandwidth level must be set before BoD services can be configured.

  If a subscription to a bandwidth level needs to be deleted or moved, all subscriptions to BoD services for subscribers in the same container must be disabled or deleted first.

- BoD services are inherited by subscribers who are subordinate in the navigation pane.

- A rule for a BoD service specifies which fields in the IP header to match—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—and the BoD service to assign to packets that match the conditions. If configured, a destination VPN can also be assigned.

  If a packet matches more than one rule for BoD services, which rule is applied is unpredictable. For example, if the destination IP address matches a rule for a Gold BoD service, but the destination port matches the source TCP port for a Silver BoD service, and the rules have no other conditions, which rule is applied is uncertain.

  Plan rules for BoD services so that a packet matches all the following conditions—protocol, source IP address, destination IP address, source TCP or UDP port, destination TCP or UDP port, or ToS byte—for only one BoD service.

Creating a Subscription to BoD Services

When you create a subscription to a BoD service, you initially set a bandwidth level if available and not previously set.

Setting a Bandwidth Level

To create a subscription to a bandwidth level:

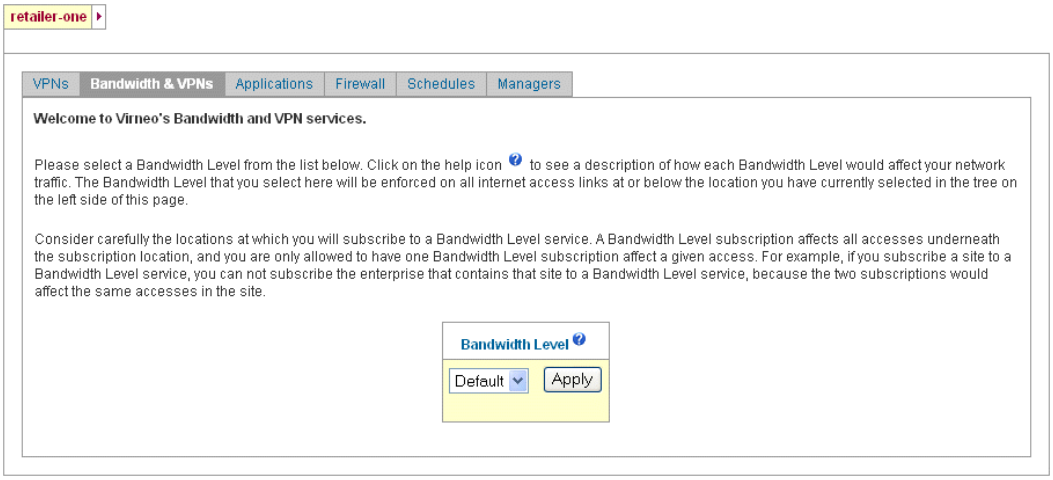
1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to provision bandwidth.

2. Click the **Bandwidth & VPNs** tab.

> **NOTE:** If VPN features are not configured, the tab is named Bandwidth.

The Bandwidth & VPNs page appears.

Figure 34: Bandwidth & VPNs Page



3. Using the field description below, select a bandwidth level, and click **Apply**.

   The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth page.

Bandwidth Level

- Bandwidth assigned to an access link (the basic BoD service in the directory). The bandwidth level governs the overall bandwidth available on the link.
- Value—Menu of bandwidth levels in the directory available for this subscriber. See the online help for information about the menu entries.
- Guidelines—A subscriber can be assigned to up to one bandwidth level on an access link.

  In the navigation pane, a subscriber subordinate to the one who has the bandwidth level subscription inherits the subscription. A subordinate subscriber cannot subscribe to another bandwidth level.

  If you select default for the value, all traffic is treated the same.

- Default—Bandwidth level specified as the default by the service provider.

Adding Subscriptions to BoD Services

To add a subscription to a BoD service:

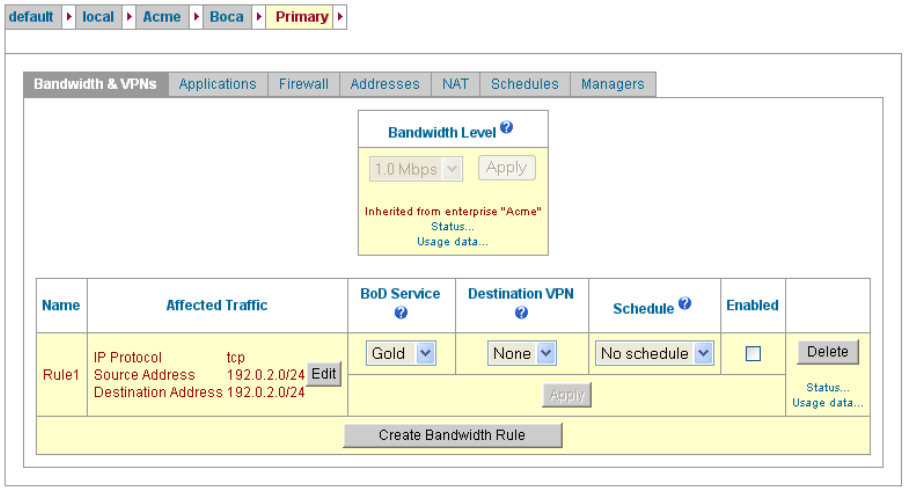
1. In the navigation pane of Enterprise Manager Portal, click the subscriber to assign to a BoD service.

2. Click the **Bandwidth & VPNs** tab.

3. If a bandwidth level has not been set, specify a bandwidth level.

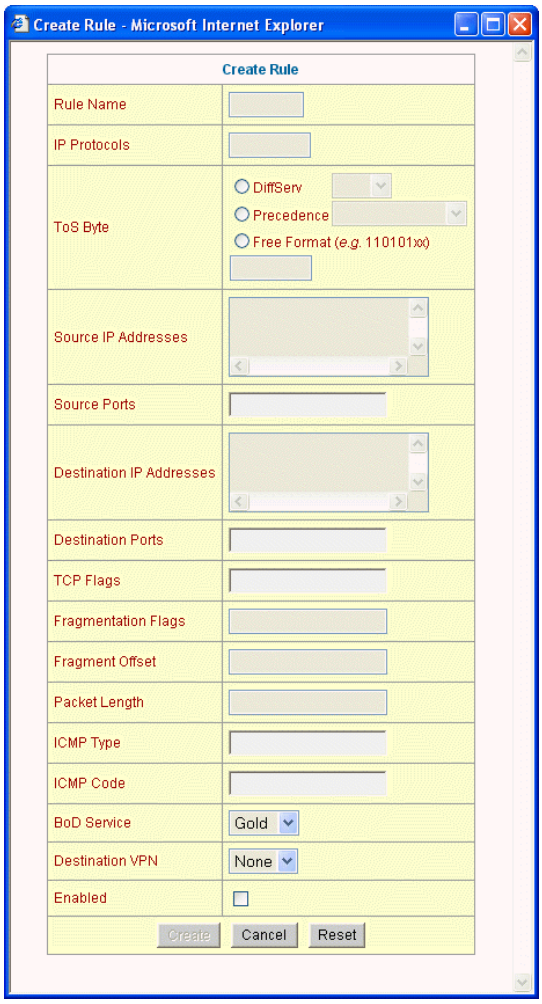
   The bandwidth level becomes available, and the fields for setting BoD services appear on the Bandwidth & VPNs page.

Figure 35: Bandwidth & VPNs Page with a Bandwidth Level Set



4. Click **Create Bandwidth Rule**.

The Create Rule dialog box appears.



5. Using the field descriptions below, configure subscriptions for BoD services.

   You can configure any number of subscriptions by assigning different traffic flows, identified by rules under Affected Traffic on the Bandwidth & VPNs page (see Figure 35 on page 477), to different BoD services.

6. Click **Create**.

   The subscription appears in the Bandwidth & VPNs page.

Rule Name

- Name of the BoD rule.
- Value—Alphanumeric characters without spaces
- Default—No value
- Example—SalesVideoConference

IP Protocols

- IP protocol associated with traffic affected by this bandwidth rule.
- Value—One of the following:
  - ah—authentication header
  - egp—exterior gateway protocol
  - esp—Encapsulating Security Payload
  - gre—generic routing encapsulation
  - icmp—Internet Control Message Protocol
  - igmp—Internet Group Management Protocol
  - ipip—IP over IP
  - ospf—Open Shortest Path First
  - pim—Protocol Independent Multicast
  - rsvp—Resource Reservation Protocol
  - sctp—Stream Control Transmission Protocol
  - tcp—Transmission Control Protocol
  - udp—User Datagram Protocol
  - < ipProtocolNumber >
- Guidelines—Specify an IP protocol or its corresponding number if you want to enable BoD for a certain type of traffic. If you want to enable BoD for all IP protocols, leave this field empty. If you specify an IP protocol other than TCP or UDP, the port fields will dim, and you will not be able to specify port numbers for this subscription.
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this bandwidth rule.
- Value
  - DiffServ—DiffServ is used to classify packets by the selected value.
  - Precedence—Value of the drop precedence.
  - Free Format—ToS byte in binary format.

    Use an x to indicate a bit to be ignored.

- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466).

  Specify the ToS byte in this field if you want to enable BoD for a specific type of service. If you want to enable BoD for all types of service, leave this field empty.

- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- Source IP address(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
  - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
  - < networkAddress > —IP address of the network
  - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not from a source IP address or not from a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty.

  The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—In this example for a JUNOS routing platform, all IP addresses on the subnet 172.16.0.0/10 are specified, except for those on the subnet 172.16.2.0/16.

  172.16.0.0/10, not 172.16.2.0/16

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Values
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
  - Ranges of port numbers separated by two dots (..)

- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(es) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value—[not] < networkAddress > / < networkMask >
  - not—Address, or set of IP addresses as expressed by the netmask, for which the BoD service is not available
  - < networkAddress > —IP address of the network
  - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify traffic not to a destination IP address or not to a set of IP addresses as expressed by the netmask, precede the IP address with the keyword **not**.

  The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.

- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this bandwidth rule.
- Value
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
  - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.

- Default—No value
- Example
  - 2
  - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

  You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

  You can use the following expression instead of the entire expression:

  - tcp-initial—syn & !ack

  The interface displays text synonyms for expressions if stored data matches the expression.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
  - syn
  - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
  - more-fragments
  - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
  - Number in the range 0–8191
  - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
  - 50
  - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
  - Number in the range 0–65536
  - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
  - 15000
  - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
  - Number of the ICMP message type in the range 0–255
  - Symbolic name for an ICMP message type
  - Comma-separated list of ICMP types and ranges of ICMP types
  - Ranges of ICMP types separated by two dots (..) within the range 0–255
  - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

  The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.
  - 0—echo-reply
  - 8—echo-request
  - 16—info-reply
  - 15—info-request
  - 18—mask-reply

- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
  - Number of ICMP code in the range 0–255
  - Comma-separated list of code numbers and ranges of code numbers
  - Ranges of code numbers separated by two dots (..) within the range 0–255
  - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

BoD Service

- Name of the BoD service in the directory that will be applied to the subscription.
- Value—Menu of BoD services available for this subscriber. See the online help for information about the menu entries.

- Guidelines—How BoD services define bandwidth allocation depends on whether or not a bandwidth level is set:
  - On a link that has a bandwidth level set, the BoD service defines the transmission service and the forwarding priority of the traffic for the subscription—for example, expedited or best-effort.
  - On a link that does not have bandwidth allocated, the BoD service typically specifies the fixed bandwidth level available to the traffic type for the subscription.

  For more information about the interaction between the bandwidth level and BoD services, see *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.
- Default—BoD service with lowest alphanumeric name in the directory
- Example—Gold

Destination VPN

- Configured VPN to use.
- Value—Name of VPN
- Guidelines—This field appears if configuration for VPNs is enabled for the portal. For more information about VPNs, see *Modifying Subscriber VPN Configuration* on page 487.
- Default—No value

Enabled

- Status of the subscription.
- Value
  - Gray box—Subscription is inherited from a parent subscriber
  - White box—Subscription is configured for this subscriber
  - Box with check mark—Subscription is enabled
  - Empty box—Subscription is disabled
- Guidelines—Click box to enable or disable a subscription.
- Default—Subscription is disabled

Modifying Rules for a Subscription to a BoD Service

To modify rules for a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Change the values in the fields for this rule.
3. Click **Apply** for the subscription.

Modifying the Bandwidth Level

To modify a bandwidth level:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select a new value from the Bandwidth Level menu.
5. Click **Apply**.
6. If needed, enable BoD services that this subscriber inherits from parent subscribers.
7. If needed, enable BoD services defined for this subscriber's subordinate subscribers.

Moving the Bandwidth Level

To move the bandwidth level to another subscriber:

1. Delete the bandwidth level. See *Deleting the Bandwidth Level* on page 486.
2. Set a bandwidth level for another subscriber. See *Creating a Subscription to BoD Services* on page 475.
3. Create BoD services. See *Creating a Subscription to BoD Services* on page 475.

Deleting a Subscription for a BoD Service

To delete a subscription to a BoD service:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Click **Delete** for the subscription.

Deleting the Bandwidth Level

To delete the bandwidth level:

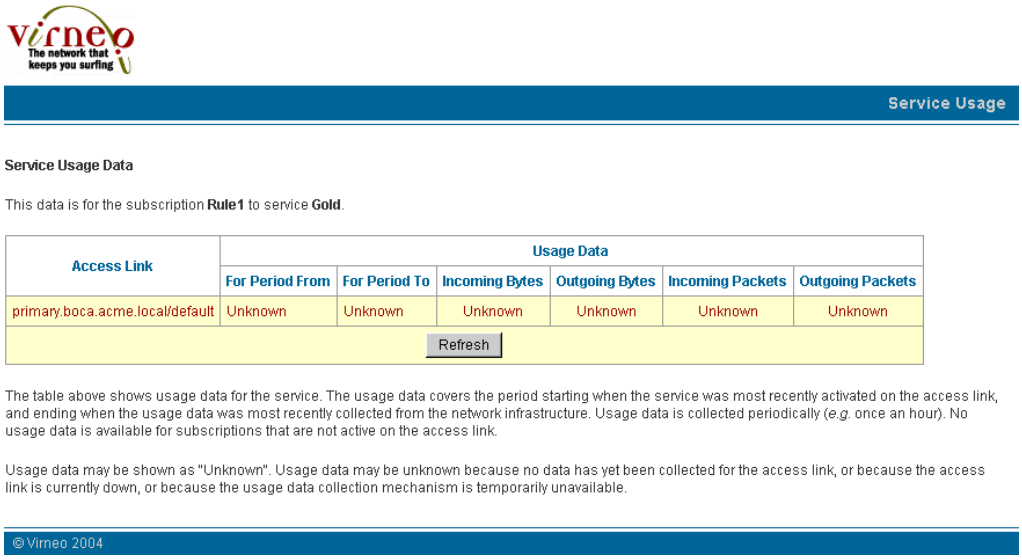
1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Disable all BoD services that this subscriber inherits from parent subscribers.
3. Disable all BoD services defined for this subscriber's subordinate subscribers.
4. Select **Default** from the Bandwidth Level menu.
5. Click **Apply**.

Monitoring Use of Subscriptions to BoD Services

To monitor the use of a bandwidth subscription:

1. Start at the subscriber's Bandwidth page (see Figure 35 on page 477).
2. Click **Usage Data** for the bandwidth level or subscription.

   The Service Usage page appears.



Integrating VPNs into an SRC Network

The service provider creates VPNs in the directory for specific subscribers. If the service provider configures the portal to display VPN features, IT managers with privileges to configure VPNs (see *Chapter 28, Managing Enterprise Service Portals*) can make modifications to VPNs that a subscriber owns.

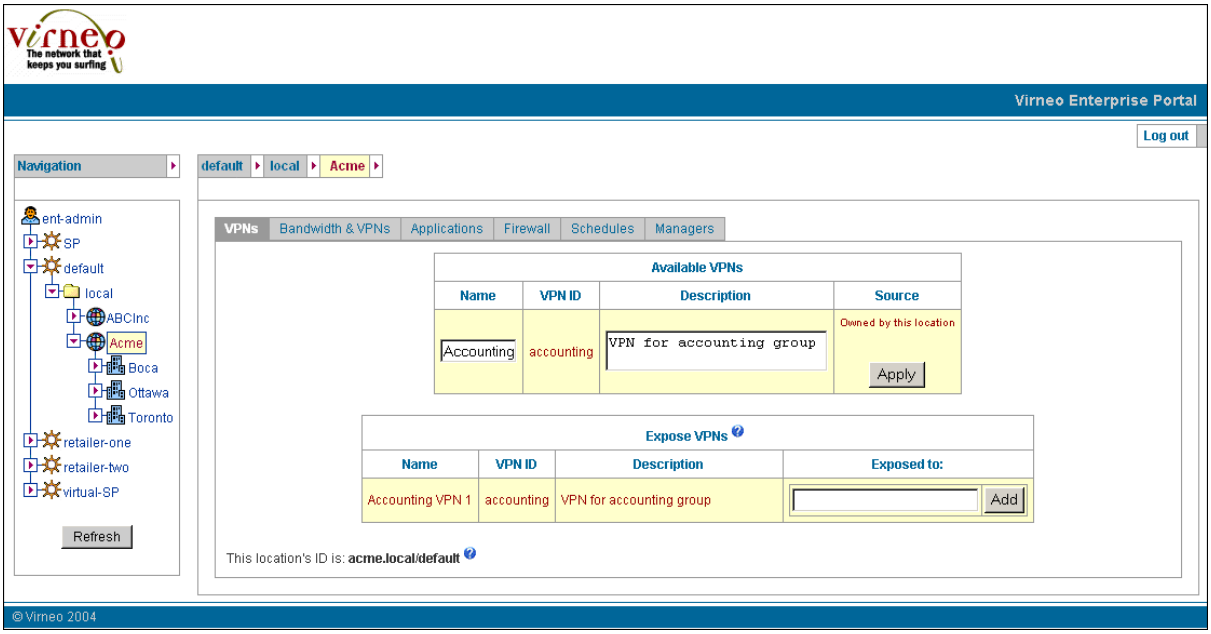
Modifying Subscriber VPN Configuration

To modify a VPN:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber who owns the VPN that you want to modify.
2. Click the **VPNs** tab.

   The VPNs page appears and displays the Available VPNs area. If the service provider configures the portal to display extranet features, this page also displays the Expose VPNs area.

Figure 36: VPNs Page



3. Using the field descriptions below, modify the VPN.
4. Click **Apply**.

Name

- Name of the VPN that appears in other pages of Enterprise Manager Portal.
- Value—Text string
- Guidelines—Enter a name that summarizes the application of this VPN.
- Default—Value of the VPN ID field
- Example—Accounting VPN

VPN ID

- Unique identifier for the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Specified by the service provider
- Example—Accounting

Description

- Description of the VPN.
- Value—Text string
- Default—Specified by the service provider
- Example—VPN for accounting in Boca

Source

- Whether or not the subscriber owns, imports, or inherits the VPN.
- Value—Text string
- Guidelines—You cannot modify this value.
- Default—Determined by the configuration of this VPN
- Example—Owned by this location

Creating Extranets

If the service provider configures the portal to display extranet features, IT managers with privileges to configure VPNs in their scope of control (see *Chapter 28, Managing Enterprise Service Portals*) can create extranets for other enterprises and retailers by exporting those VPNs. Enterprises and retailers who share VPNs that other subscribers own are called *extranet clients*.

To create an extranet:

1. Obtain a location identifier from the extranet client.

   When you click an enterprise or retailer in the navigation pane of Enterprise Manager Portal, the location identifier for that subscriber appears at the bottom of the VPNs page (see Figure 36 on page 488). The default format of the location identifier is:

   [< enterpriseName > . < subscriberFolderName > /] < retailerName >

   - enterpriseName—Name of the enterprise in the directory
   - subscriberFolderName—Name of the subscriber folder that contains the directory
   - retailerName—Name of the retailer in the directory

2. Start at the VPN page for the subscriber who owns the VPN.
3. In the field called Exposed to in the Expose VPNs area, enter the location identifier for the extranet client.
4. Click **Add**.

   The VPN page for the subscriber who owns the VPN displays the updated status of the VPN, and the extranet client now has access to the VPN.

Deleting Extranets

You can delete an extranet by canceling the export of a VPN. To do so:

1. Start at the VPN page for the subscriber who owns the VPN.
2. In the Expose VPNs area, identify the VPN and the extranet client for whom you want to delete the extranet.

3. Click **Delete** for the extranet client in the field Exposed to.

   This action will deactivate all subscriptions to this VPN for the extranet client, and the extranet client will not be able to reactivate subscriptions to the VPN.

Sending Traffic to a VPN

If the service provider makes VPN features visible to subscribers, the name of the Bandwidth tab in the portal changes to Bandwidths & VPNs, and you can send traffic associated with BoD services to VPNs. To do so:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to send traffic to a VPN.

2. Click the **Bandwidth and VPNs** tab.

3. Follow the instructions in *Managing Subscriptions to Bandwidth-on-Demand Services* on page 474 to configure the BoD service.

4. From the menu in the Destination VPN field for that subscription, select the VPN to which you want to send the traffic.

5. Click **Create** for the subscription.

Modifying the VPN to Which the Router Sends Traffic

To modify the VPN to which the router sends traffic:

1. Start at the subscriber's Bandwidth & VPN page (see Figure 34 on page 476).

2. From the menu in the Destination VPN field for the subscription, select a different VPN from the menu.

3. Click **Apply** for the subscription.

Stopping the Router from Sending Traffic to VPNs

To stop a router from sending traffic to a VPN:

1. Start at the subscriber's Bandwidth & VPNs page (see Figure 34 on page 476).
2. From the menu in the Destination VPN field for the subscription, select **None**.
3. Click **Apply** for the subscription.

Classifying Traffic for Stateful Firewall Exceptions and NAT Rules

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception to a stateful firewall or by a NAT rule. These application objects are based on application protocols—protocols that are categorized in the application layer of the TCP/IP reference model—or IP protocols that the JUNOS routing platform supports. Subordinate subscribers inherit application objects configured for parent subscribers.

An application protocol defines how a client and a server communicate during a *conversation*—a particular activity between the client and the server, such as an FTP session. A conversation in the application layer consists of multiple *flows*. A flow is one element of the conversation; for example, in an FTP session, the initial TCP control connection or a subsequent UDP traffic connection. You can apply a NAT rule or a firewall exception to the initial flow in a conversation by defining an application object. The NAT rule or firewall exception then applies to all subsequent flows in that conversation.

In the FTP example, the client may create a TCP connection to the server and send the server a UDP port number in the initial flow. The server may then start sending UDP traffic to the UDP port specified in the initial flow. If the initial flow matches a defined application object that a firewall allows, the firewall will allow the UDP traffic in the second flow and in all subsequent flows in the conversation.

Certain application protocols, such as FTP, are supported explicitly, and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for an application protocol that is not explicitly supported, such as HTTP, you can create an application object based on an IP protocol only. For example, you could create an application object called HTTP, specify no application protocol, and select TCP as the IP protocol. You can then specify 8080 for the source and destination ports in the application protocol to identify the HTTP traffic.

Classifying Traffic

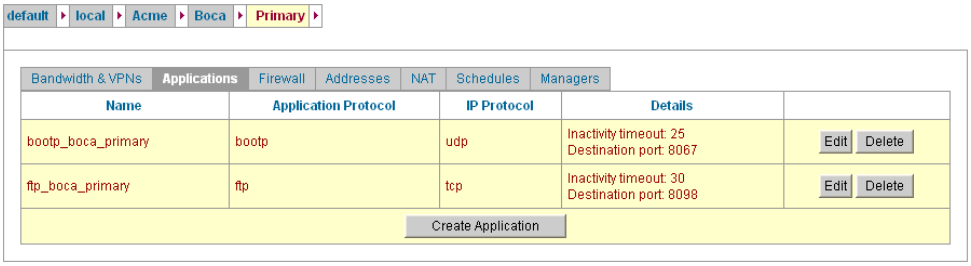
To create an application protocol:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber to whom you want to assign the application object.

2. Click the **Applications** tab.

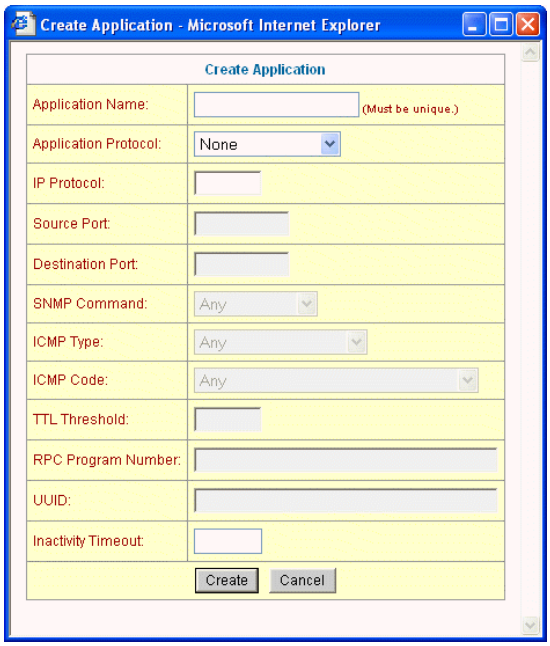
   The Applications page appears. This page displays the application protocols that the subscriber inherits from parent subscribers and application protocols configured explicitly for the subscriber.

Figure 37: Applications Page



3. Click **Create Application**.

   The Create Application page appears.



4. Using the following field descriptions, specify details for the application protocol.

   Some fields are available only for certain applications. When a field is unavailable, the box in which you enter information is dimmed, and you cannot enter information in it.

5. Click **Apply**.

Application Name

- Name for this application protocol.
- Value—Text string
- Default—No value
- Example—bootp-boston

Application Protocol

- Application protocol.
- Value—Type of application protocol or None
- Guidelines—Select a protocol from the menu to specify that the application uses a particular application protocol. Depending on the application protocol you choose, some fields in the application object are irrelevant (and disabled) or restricted to specific values. If the application protocol you want is not available, you can select the option **None** and base the application object on an IP protocol. If you select this option, the NAT rule or firewall exception affects only the first flow in a conversion. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.
- Default—Any
- Example—bootp

IP Protocol

- IP protocol.
- Value—Type of IP protocol or number of IP protocol in the range 0–255
- Guidelines—The names of the allowed IP protocols are shown in the tool tips for this field. The portal automatically selects an IP protocol for certain application protocols.
- Default—No value
- Example—tcp

Source Port

- Source TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

Destination Port

- Destination TCP/UDP ports (as contained in the IP packets) of traffic for this application object.
- Value—Integer in the range 0–65535
- Guidelines—Enter either a single port number or a range of port numbers separated by two dots (..). To specify all ports, leave this field empty.
- Default—No value
- Example—25..35

SNMP Command

- Type of command for Simple Network Management Protocol (SNMP).
- Value—Type of SNMP command
- Guidelines—Select a type of command from the menu.
- Default—Any
- Example—get-next

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message
- Guidelines—Select a type of message from the menu.
- Default—Any
- Example—info-reply

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code
- Guidelines—Select a type of code from the menu.
- Default—Any
- Example—host-precedence-violation

TTL Threshold

- Depth of network penetration for the traceroute application protocol.
- Value—Integer in the range 0–255 or unspecified
  - Unspecified—Allows traceroutes up to a depth of 255.
- Default—Unspecified
- Example—5

RPC Program Number

- Program number for the remote procedure call (RPC) application protocol.
- Value—A single program number or range of program numbers separated by two dots (..). Program numbers are integers in the range 100000–400000.
- Guidelines—Specify the RPC program numbers to which the NAT rule or firewall exception applies. To specify all RPC program numbers, leave this field empty.
- Default—No value
- Example—7..12

UUID

- Universal unique identifier (UUID) for the Distributed Computing Environment (DCE) RPC application protocol.
- Value—Hexadecimal number in the format xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
- Guidelines—Specify a number of a specific DCE RPC object to which the NAT rule or firewall exception applies. To specify all DCE RPC objects, leave this field empty.
- Default—No value
- Example—1f356a25-ce67-73ad-2187-631ec8ae1bd6

Inactivity Timeout

- Time for which a conversation associated with the identified application protocol can be inactive before the JUNOS routing platform terminates the conversation.
- Value—Number of seconds in the range 0–2147483647
- Guidelines—Specify a time, or leave this field empty to use the default setting.
- Default—30 seconds
- Example—45

Modifying Values for Traffic Classifications

To modify values for an application object:

1. Start at the Applications page (see Figure 37 on page 492).
2. Click **Edit** for the application object.

   The Edit Application page appears.
3. Change the values in the fields for this application object.
4. Click **Apply**.

Deleting Traffic Classifications

To delete an application protocol:

1. Start at the Applications page (see Figure 37 on page 492).
2. Click **Delete** for the application protocol.

Subscribing to Firewall Services

The basic firewall that you configure will be enforced on all Internet access links subordinate to the subscriber you select in the navigation pane. When you have configured a basic firewall, you can create firewall exceptions—variances from the basic firewall—for specific categories of traffic.

Firewall exception rules block traffic that otherwise would be permitted to traverse the firewall, or to admit traffic that would otherwise be blocked. Exceptions specify criteria against which each packet is inspected.

How you configure firewall exceptions depends on which type of firewall service the ISP enabled. Enterprise Manager Portal can support one of the following:

- Stateless firewalls—Inspect each packet in isolation; they do not evaluate the traffic flow.

  With stateless firewalls, you can configure exceptions to take customized actions, such as policing specified traffic at a specified rate, or setting the ToS byte. By using customized actions, you can allow traffic from a specified IP address or for a specified IP protocol to traverse the firewall. In addition, you can specify quality of service (QoS) properties such as values for the type of service (ToS) byte.
- Stateful firewalls—Track traffic flows and conversations between applications and evaluate this information when applying exception rules.

An application is typically associated with a stateful firewall rule. After a flow or conversation meets firewall criteria, packets in that flow can pass through the firewall. For example for an FTP connection, when an FTP control connection requests a file download, the stateful firewall knows to expect and allows a TCP data connection to start. You can also create firewall exceptions for traffic associated with a particular application protocol, such as FTP, that originates at a particular address in the enterprise. See *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491 for information about defining an application object, which defines traffic associated with a particular application protocol.

Before You Configure Firewall Exception Rules

Before you configure firewall exception rules, make sure that you understand which types of packets you want to pass through a firewall.

Enterprise Manager Portal must be set to Advanced configuration mode to configure some of the properties for a firewall. If the portal is not in Advanced mode, some of the settings appear as read-only fields. For information about setting the portal mode, see *Setting the Configuration Level for Enterprise Manager Portal* on page 466.

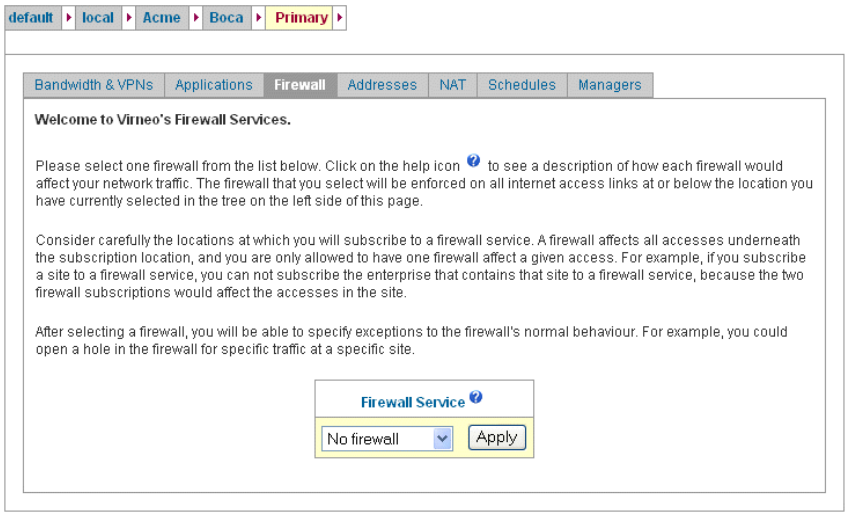
Creating Subscriptions to Firewall Services

To create a subscription to a basic firewall service:

1. In the navigation pane of Enterprise Manager Portal, click the subscriber for whom you want to create a subscription to a basic firewall service.

2. Click the **Firewall** tab.

   The Firewall page appears.



3. Click the help icon above the firewall service to review information about the available firewalls.

4. Select a firewall service from the menu, and click **Apply**.

   The Firewall page changes to allow you to create firewall exceptions.

Firewall Service

- Name of the firewall service.
- Value—Menu of firewall services in the directory available for this subscriber
- Default—No Firewall
- Example—BasicFW1

Creating Firewall Exceptions for Stateless Firewalls

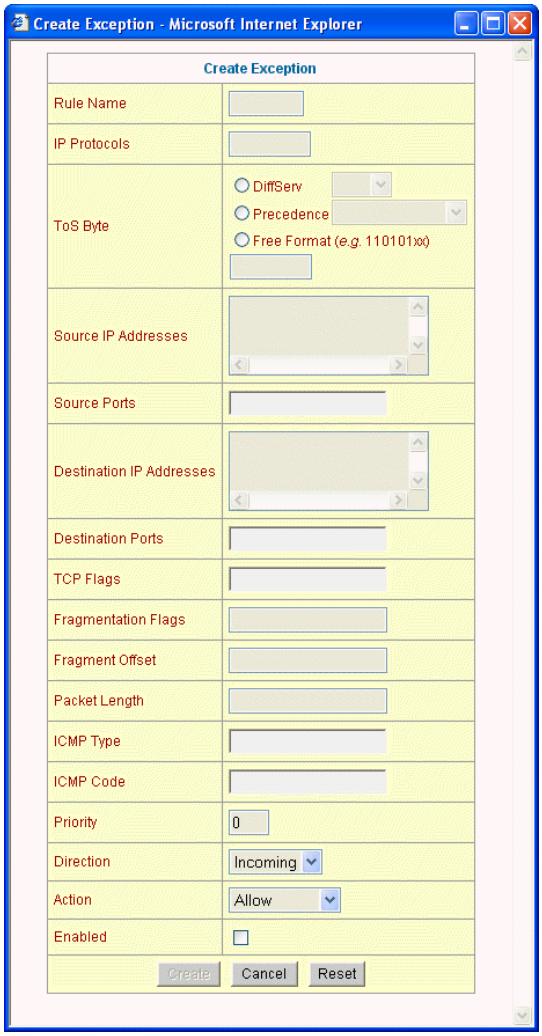
To create a firewall exception for a subscriber:

1. Access the subscriber's Firewall page (see Figure 40 on page 508).

2. In the Firewall page, click **Create Firewall Exception**.

   The Create Exception dialog box appears. Figure 38 shows the appearance of the dialog box when Enterprise Manager Portal is set to Advanced mode.

Figure 38: Create Exception Dialog Box for Stateless Firewalls



Using the field descriptions below, configure the values for the firewall exception. Which protocols you select determines which associated protocol fields are available for editing.

NOTE: If a user changes the value for a protocol when the configuration level for the portal is set to Normal mode, values for the following fields may be deleted: TCP Flags, Fragmentation Flags, Fragmentation Offset, Packet Length, ICMP Type, and ICMP Code.

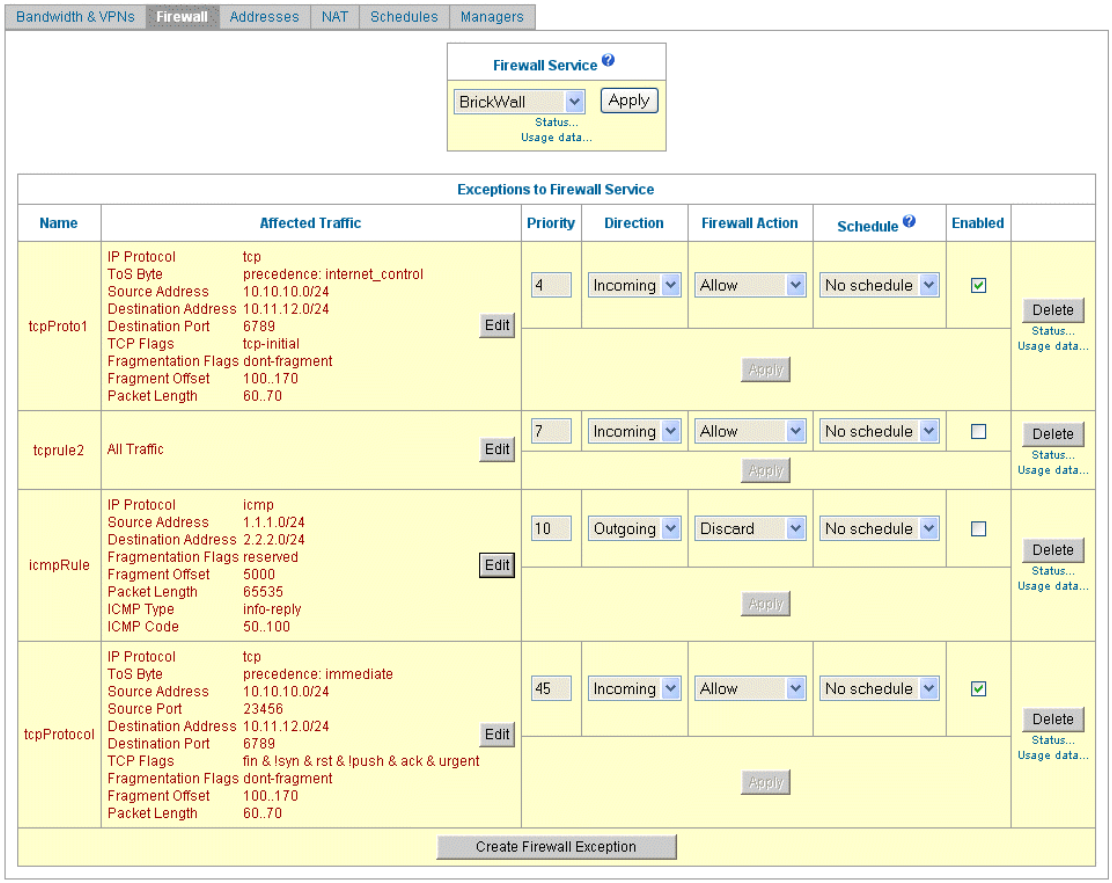
If the value of a protocol is changed to the original setting, the portal restores the associated field values that were previously removed.

---

3. Click **Create**.

   The Firewall page shows the exception configured. Figure 39 shows three exceptions configured for a brickwall firewall service. The exceptions appear in priority order.

Figure 39: Firewall Page with Firewall Service Applied and Exceptions Configured



Rule Name

- Name of the subscription to the firewall service.
- Value—Alphanumeric string
- Guidelines—You must specify a name for the rule. Do not use spaces, dots, or punctuation characters in the name.
- Default—No value
- Example—WebAccess

IP Protocols

- IP protocol associated with this rule.
- Value—Type of IP protocols separated by commas, with the protocol specified by:
  - Number of IP protocol in the range 0–255
  - The following abbreviations:
    - ah—authentication header
    - egp—exterior gateway protocol
    - esp—Encapsulating Security Payload
    - gre—generic routing encapsulation
    - icmp—Internet Control Message Protocol
    - igmp—Internet Group Management Protocol
    - ipip—IP over IP
    - ospf—Open Shortest Path First
    - pim—Protocol Independent Multicast
    - rsvp—Resource Reservation Protocol
    - sctp—Stream Control Transmission Protocol
    - tcp—Transmission Control Protocol
    - udp—User Datagram Protocol
  - Blank—Any IP protocol
- Default—No value
- Example—tcp

ToS Byte

- ToS byte in the header of the IP datagram associated with traffic affected by this rule.
- Value
  - DiffServ—DiffServ is used to classify packets by the selected value.
  - Precedence—Value for the drop precedence.
  - Free Format—ToS byte in binary format.

    Use an x to indicate a bit to be ignored.
- Guidelines—You can configure the ToS byte only if the configuration level is set to Advanced.

  Specify the ToS byte in this field if you want to specify a specific type of service. If you want to specify all types of service, leave this field empty.
- Default—No value
- Example—Free Format 000010xx

Source IP Addresses

- IP addresses (as contained in the IP packets) of traffic to which the rule applies.
- Value—[not] < networkAddress > / < networkMask >
  - not—All addresses except the listed addresses
  - < networkAddress > —IP address of the network
  - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, enter multiple addresses on different lines. You can specify multiple source IP addresses only if the configuration level is set to Advanced.
- Default—No value
- Example—192.0.2.0/24

Source Ports

- Source TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Values
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
  - Ranges of port numbers separated by two dots (..)
- Guidelines— To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

Destination IP Addresses

- Destination IP addresse(es) (contained in the IP packets) of traffic affected by this rule.
- Value—[not] < networkAddress > / < networkMask >
  - not—Address, or set of IP addresses as expressed by the netmask, for which the firewall service is not available
  - < networkAddress > —IP address of the network
  - < networkMask > —Netmask expressed as an integer 0–32, which specifies how many of the first bits in the address specify the network
- Guidelines—To specify a netmask for a destination IP address or a set of IP addresses that should not be included, precede the IP address with the keyword **not**. The order in which you list prefixes, identified by the IP address–netmask pair, is not significant. They are all evaluated to determine whether a match occurs. If prefixes overlap, longest-match rules are used to determine whether a match occurs. For an address to be considered a match, it must match one of the rules in the list.

  For information about how JUNOS routing platforms evaluate prefixes, see the *JUNOS Policy Framework Configuration Guide*.
- Default—No value
- Example—192.0.2.0/24

Destination Ports

- Destination TCP/UDP port(s) (contained in the IP packets) of traffic affected by this rule.
- Value
  - Port number
  - Comma-separated list of port numbers and ranges of port numbers (JUNOS routing platforms)
  - Ranges of port numbers separated by two dots (..)
- Guidelines—To specify all ports, leave this field empty. If you specify an IP protocol other than TCP or UDP for this subscription, the port field will dim, and you will not be able to specify port numbers in this field.
- Default—No value
- Example
  - 2
  - 2, 3, 45..55

TCP Flags

- Conditions in the TCP flags in the TCP message header. This field is enabled when the TCP protocol is selected.
- Value—Expression or text synonym that identifies the TCP flags
- Guidelines—You can enter a value for TCP flags only if you select TCP as the IP protocol.

  You can enter a logical expression that contains the symbols for the six TCP flags: urgent, ack, push, rst, syn, and fin. You can use the following logical operators in the list of flags:

  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.

  You can use the following expression instead of the entire expression:

  - tcp-initial—syn & !ack

  The interface displays text synonyms for expressions if stored data matches the expression.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—No value
- Example
  - syn
  - tcp-initial

Fragmentation Flags

- Logical expression using the dont-fragment, more-fragments, and reserved IP fragmentation flags.
- Value—Flags expression
- Guidelines—The expression can also contain the following logical operators:
  - &—And. Separates flag settings in the list.
  - !—Not. Flags preceded by ! are cleared; flags not preceded by ! are set.
- Default—No value
- Example
  - more-fragments
  - ! dont-fragment

Fragment Offset

- IP fragment offset—a value that defines the order in which to assemble fragments for an IP datagram.
- Value—One of the following:
  - Number in the range 0–8191
  - Range of numbers separated by two dots (..) within the range 0–8191
- Default—No value
- Example
  - 50
  - 50 .. 76

Packet Length

- Length of packets.
- Value—One of the following:
  - Number in the range 0–65536
  - Range of numbers separated by two dots (..) within the range 0–65536
- Default—No value
- Example
  - 15000
  - 15000 .. 30000

ICMP Type

- Type of message for Internet Control Management Protocol (ICMP).
- Value—Type of ICMP message in the following formats:
  - Number of the ICMP message type in the range 0–255
  - Symbolic name for an ICMP message type
  - Comma-separated list of ICMP types and ranges of ICMP types
  - Ranges of ICMP types separated by two dots (..) within the range 0–255
  - Blank—Any ICMP type
- Guidelines—You can enter a value for this field only if you select the icmp protocol (protocol number 1).

  The following list shows the symbolic name and associated numbers for ICMP types. The ICMP types are the same as those on JUNOS routing platforms with the addition of traceroute.
  - 0—echo-reply
  - 8—echo-request
  - 16—info-reply
  - 15—info-request
  - 18—mask-reply

- 17—mask-request
- 12—parameter-problem
- 5—redirect
- 9—router-advertisement
- 10—router-solicit
- 4—source-quench
- 11—time-exceeded
- 13—timestamp
- 14—timestamp-reply
- 30—traceroute
- 3—unreachable

This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—10 .. 25, 27

ICMP Code

- Code for ICMP.
- Value—Type of ICMP code in the following formats:
  - Number of ICMP code in the range 0–255
  - Comma-separated list of code numbers and ranges of code numbers
  - Ranges of code numbers separated by two dots (..) within the range 0–255
  - Blank—Any ICMP code
- Guidelines—You can enter a value for this field only if you select particular protocols.

  This field appears enabled only if the configuration level is set to Advanced. Although the value can be changed when the configuration level is set to Normal, we recommend that the value of this field not be changed if the field appears disabled.

- Default—Any
- Example—75

Priority

- Numeric value that indicates which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field

- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Direction

- Direction, with respect to the enterprise, of the traffic.
- Value
  - Incoming—Applies to traffic that starts outside the enterprise
  - Outgoing—Applies to traffic that starts inside the enterprise
  - Both—Applies to traffic flows that start inside or outside the enterprise
  - Guidelines—If you select a custom firewall rule, you cannot specify a direction. Custom firewall rules should have names that reflect what the rule does.
- Default—Incoming
- Example—Both

Action

- Way in which the firewall should handle the incoming or outgoing traffic.
- Value
  - Allow—Let the traffic through the firewall.
  - Reject—Send an ICMP reply that explains why the firewall blocked the traffic.
  - Discard—Drop the traffic without sending any reply.
  - A custom value configured by the service provider.
- Guidelines—Other actions may be available—one for each custom firewall rule.
- Default—Allow
- Example—Discard

Enabled

- Status of the rule.
- Value
  - Gray box—Rule is inherited from a parent subscriber or the rule is scheduled
  - White box—Rule is configured for this subscriber
  - Box with check mark—Rule is enabled
  - Empty box—Rule is disabled
- Guidelines—Click box to enable or disable a rule.
- Default—Rule is disabled

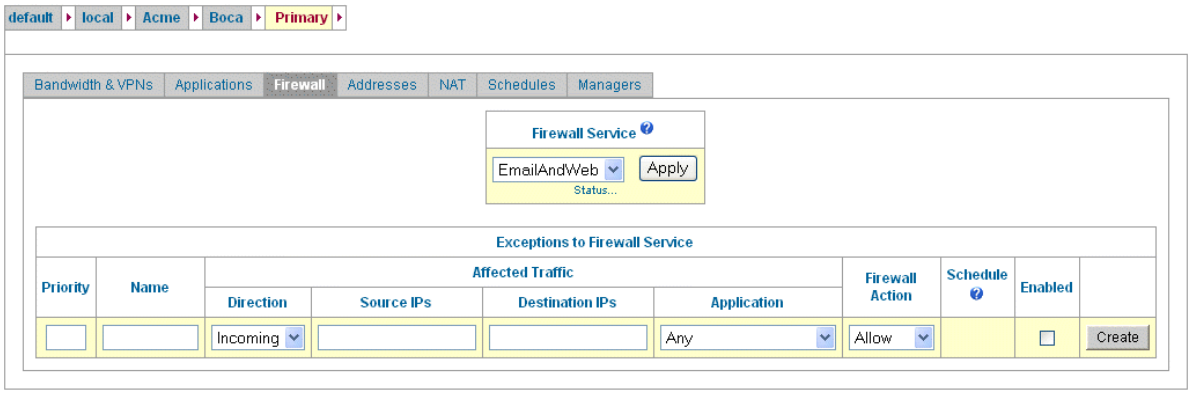
Creating Firewall Exceptions for Stateful Firewalls

To create a firewall exception for a subscriber:

1. If you want to create a firewall exception for a particular application object, first create that object (see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491).

2. Access the subscriber's Firewall page.

Figure 40: Firewall Page with Firewall Service Applied



3. Using the field descriptions below, configure the values for the firewall exception.

4. Click **Create**.

Priority

- Numeric value to indicate which firewall exception takes precedence if a subscriber has multiple exceptions for a firewall service.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the firewall exception. A lower number indicates a higher priority. Use a unique priority for each firewall exception that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.
- Default—No value
- Example—5

Name

- Name of the subscription to the firewall service.
- Value—Text string
- Guidelines—You must specify a name for the firewall exception.
- Default—No value
- Example—videoConference

Direction

- Direction, with respect to the enterprise, of the initial traffic flow in a conversation.
- Value
  - Incoming—Applies to an initial traffic flow that starts outside the enterprise
  - Outgoing—Applies to an initial traffic flow that starts inside the enterprise
  - Both—Applies to initial traffic flows that start inside or outside the enterprise
- Default—Incoming
- Example—Both

Source IPs

- Source IP addresses (as contained in the IP packets) of traffic to which the firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
  - not—All addresses except the listed addresses
  - < networkAddress > —IP address of the network
  - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular source IP address, enter an IP address. To specify all traffic except that with a particular source IP address, precede the IP address with the keyword **not**. To specify traffic with any source IP address, leave the field empty. To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Destination IPs

- Destination TCP/UDP ports (as contained in the IP packets) of traffic to which this firewall exception applies.
- Value—[not] < networkAddress > / < networkMask >
  - not—All addresses except the listed addresses
  - < networkAddress > —IP address of the network
  - < networkMask > —Subnet mask
- Guidelines—To specify traffic with a particular destination IP address, enter an IP address. To specify all traffic except that with a particular destination IP address, precede the IP address with the keyword **not**. To specify multiple destination IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466), and enter multiple addresses on different lines.
- Default—No value
- Example—192.0.2.0/24

Application

- Application object to which the firewall applies.
- Value—Application object you defined
- Guidelines—Select an application object from the menu. For information about specifying an application object, see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491.
- Default—Any
- Example—ftp

Firewall Action

- The way in which the firewall should handle the incoming or outgoing traffic.
- Value
  - Allow—Let the traffic through the firewall
  - Reject—Send an ICMP reply that explains why the firewall blocked the traffic
  - Discard—Drop the traffic without sending any reply
- Default—Allow
- Example—Discard

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal. For more information about schedules, see *Managing Schedules* on page 467.
- Default—No value

Enabled

- Status of the firewall exception.
- Value
  - Gray box—Firewall exception is inherited from a parent subscriber
  - White box—Firewall exception is configured for this subscriber
  - Box with check mark—Firewall exception is enabled
  - Empty box—Firewall exception is disabled
- Guidelines—Click box to enable or disable a firewall exception.
- Default—Firewall exception is disabled

Adding a Schedule to a Firewall Exception

A schedule must be configured before you can apply one to a firewall exception. For information about configuring schedules in Enterprise Manager Portal, see *Managing Schedules* on page 467.

To add a schedule to a firewall exception:

1. Access the subscriber's Firewall page (see Figure 39 on page 500).
2. In the Firewall page, select a schedule from the Schedule menu for the exception. See the following field description for details.

Schedule

- Configured schedule to use.
- Name of the schedule
- Guidelines—This field appears if scheduling is enabled for the portal.
- Default—No value

Modifying Firewall Exceptions

To modify a firewall exception:

1. Start at the Firewall page for the subscriber (see Figure 40 on page 508).
2. Change the values in the fields for this firewall exception.
3. For stateless firewalls, to change the values for affected traffic, click Edit under Affected Traffic, make changes in the Edit Exception dialog box, and click **Apply**.

   or

   For stateful firewalls, click **Apply** for the application protocol.

Deleting Firewall Exceptions

To delete a firewall exception:

1. Start at the Firewall page for the subscriber (see Figure 40 on page 508).
2. Click **Delete** for the firewall exception.

Deleting Basic Firewalls

To delete a basic firewall:

1. Disable all firewall exceptions and NAT rules configured for this subscriber.

   For information about disabling these values, see the field descriptions in *Creating Firewall Exceptions for Stateful Firewalls* on page 508 and *Applying NAT Rules to Traffic* on page 516.

2. Disable all firewall exceptions and NAT rules that this subscriber inherits from parent subscribers.

3. Disable all firewall exceptions and NAT rules defined for this subscriber's subordinate subscribers.

4. Access the Firewall page for the subscriber for which you configured the firewall (see Figure 40 on page 508).

5. Select **No Firewall** from the Firewall Service menu.

6. Click **Apply**.

Monitoring the Use of Subscriptions to Firewall Services

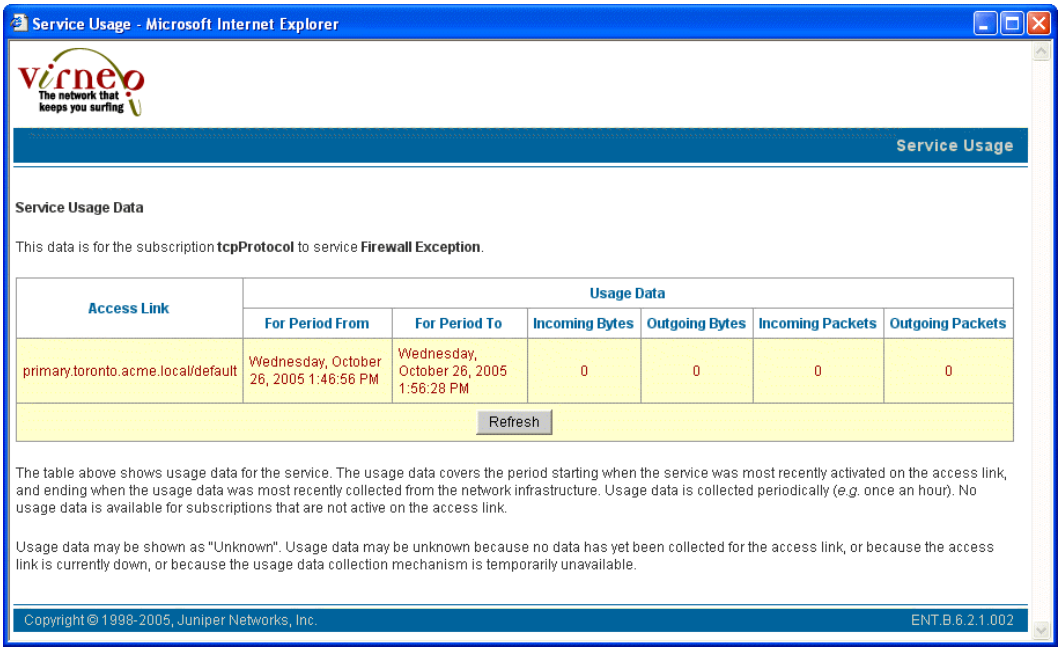
To monitor the use of firewall subscriptions:

1. Access the subscriber's Firewall page (see Figure 40 on page 508).
2. In the Firewall page, click the **Usage Data** link in the last column.

   or

   Click the **Usage Data** link under Firewall Service.

   The Service Usage Data page appears.



Working with IP Addressing and NAT Services

You can configure NAT addressing and services from Enterprise Manager Portal. For information about NAT services and policies, see *Chapter 22, Reviewing and Configuring Policies and Services for Enterprise Manager Portal*.

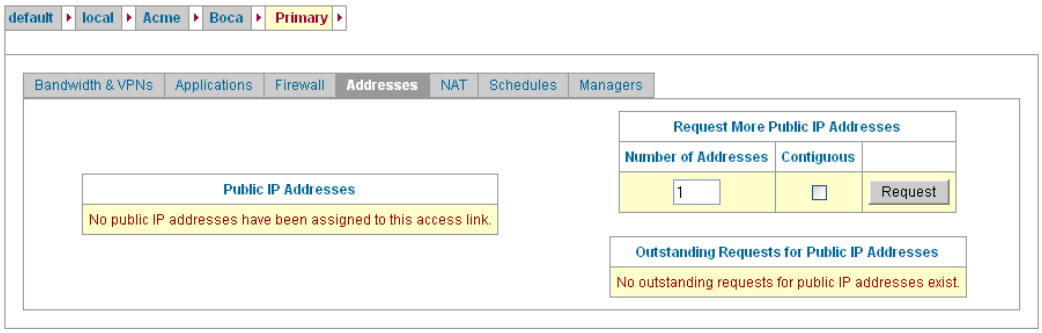
Requesting Public IP Addresses for NAT Services

To request one or more IP addresses:

1. In the navigation pane of Enterprise Manager Portal, click the access to which you want to request an IP address.
2. Click the **Addresses** tab.

The Addresses page appears.

Figure 41: Addresses Page Before Requesting Addresses



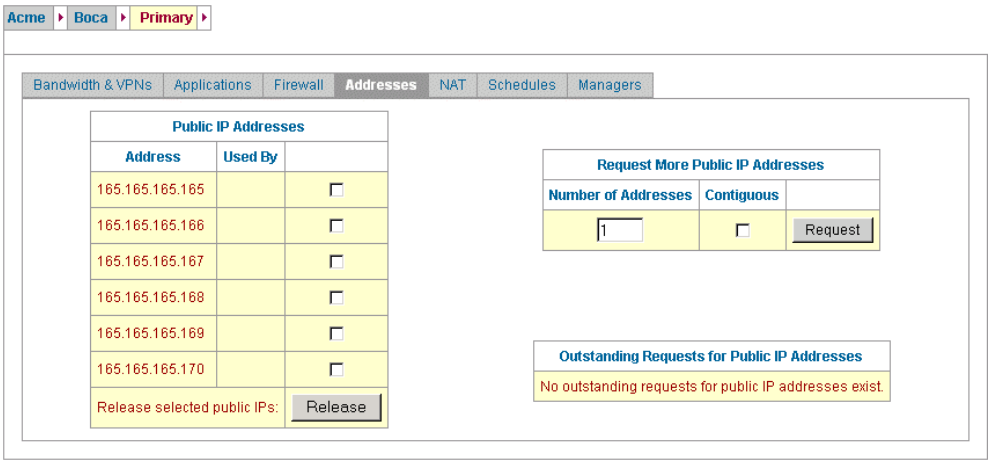
3. In the Number of Addresses field, enter the number of addresses that you want.

4. (Optional) If you specify multiple IP addresses and you want the addresses to be sequential, select **Contiguous**.

5. Click **Request**.

   Enterprise Manager Portal sends a request to the service provider for the IP addresses and displays the number of outstanding requests. When the service provider allocates the IP addresses, Enterprise Manager Portal displays the public IP addresses assigned to this access and makes the addresses visible in the menus on the NAT page for that access, as shown in Figure 42 on page 514. If a request for an IP address is outstanding for a certain period of time, Enterprise Manager Portal automatically sends a reminder to the service provider.

Figure 42: Addresses Page After Requesting Addresses



Number of Addresses

- Number of IP addresses that you want the service provider to supply.
- Value—Integer in the range 1–2147483647
- Default—1

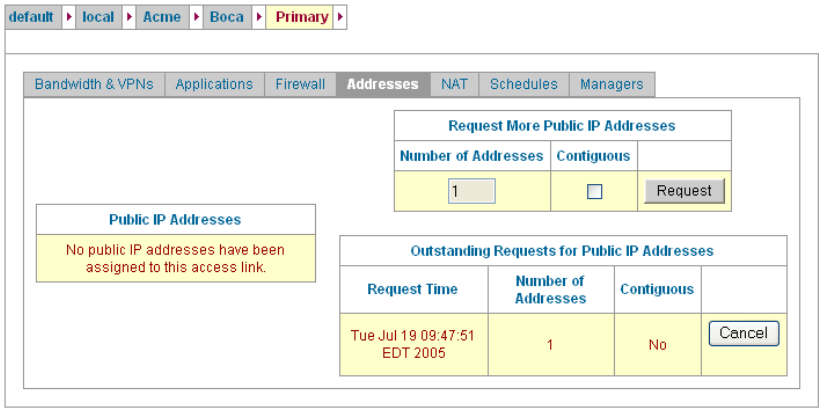
Contiguous

- Whether or not requested multiple IP addresses should be sequential.
- Value
  - Checked box—IP addresses must be contiguous
  - Empty box—IP address need not be contiguous
- Default—IP address need not be contiguous

Canceling Requests for Public IP Addresses

To cancel a request:

- Click **Cancel** for that request in the Outstanding Requests for IP Addresses table.



Returning Public IP Addresses to Service Providers

To return one or more IP addresses to the service provider:

1. Start at the Addresses page for the subscriber (see Figure 42 on page 514).
2. In the Public IP Addresses table, click in the small box in the last column for each address that you want to return.

   If an enabled NAT rule is using an address, the box for that address is dimmed, and you cannot release that address until you disable or delete the NAT rule listed in the Used By field.
3. Click **Release**.

Applying NAT Rules to Traffic

After you protect an access with a firewall and have obtained one or more public IP addresses for the access, you can apply the following types of NAT rules to traffic on the access.

- Public addresses for outgoing traffic

  Also known as *dynamic source NAT*, this type of NAT allows computers with private IP addresses in a private network to share a small set of public IP addresses for outgoing connections. For example, employees in an enterprise can use these public IP address for browsing the Web. You can specify the source IP addresses and, optionally, the ports that the outgoing traffic will use.

- Public addresses for incoming traffic

  Also known as *static destination NAT*, this type of NAT allows you to expose to the world a server, such as a Web server, that has a private IP address in your private network. You specify a public IP address, and incoming connections destined for that public IP address will be received by your server at its private IP address.

- Fixed public addresses for outgoing traffic

  Also known as *static source NAT*, this type of NAT allows you to specify the public source IP to be used for specific outgoing traffic. To specify this type of NAT you must set the configuration level of the portal to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466*)*.

Enterprise Manager Portal ensures that the SAE activates a basic firewall service before it activates a NAT service.

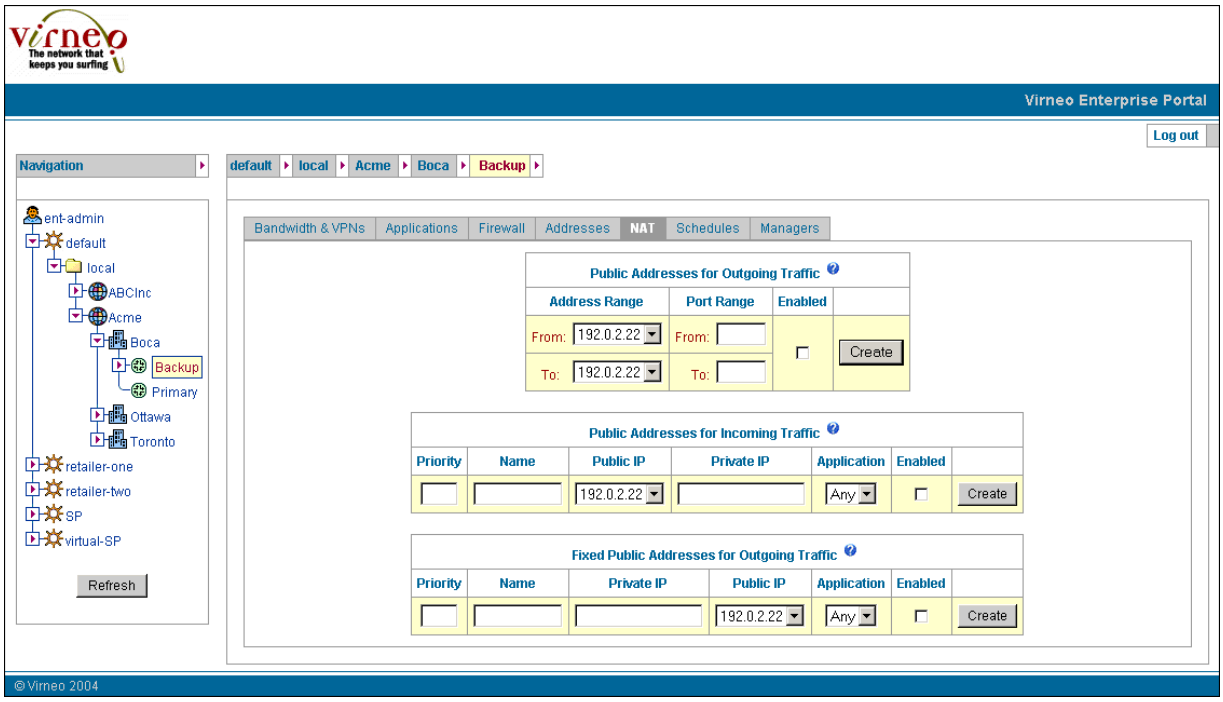
To apply NAT rules to traffic on JUNOS routing platforms:

1. In the navigation pane of Enterprise Manager Portal, click the access that connects to the router.

2. Click the **NAT** tab.

   The NAT page appears.

Figure 43: NAT Page



3. See the following sections for information about configuring NAT for incoming and outgoing interfaces on the router.

Configuring Public IP Addresses for Outgoing Traffic

To configure public IP addresses for outgoing traffic:

1. Locate the area called Public Addresses for Outgoing Traffic in the NAT page.

2. Using the field descriptions below, specify how the router will apply the NAT rule to outgoing traffic.

3. Select **Enabled**.

4. Click **Create**.

Address Range

- Contiguous range of public IP addresses to which the source addresses of clients in the enterprise are translated.
- Value—Public IP addresses
- Guidelines—Select the starting and ending IP addresses in the From and To menus. For one IP address, select the same address in the From and To menus.
- Default—No value

Port Range

- Range of ports that are used as the source ports in outgoing IP packets after the NAT translation.
- Value—Integers in the range 0–65535
- Guidelines—Specify the starting and ending port numbers in the From and To fields. Be sure to use a port range big enough to allow all the private addresses to share the limited set of public addresses. To specify all ports in the range 1024–65535, leave these fields empty.
- Default—No value

Enabled

- Whether or not the router applies NAT to outgoing traffic on this access.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Configuring Public IP Addresses for Incoming Traffic

To configure public IP addresses for incoming traffic:

1. Locate the area called Public Addresses for Incoming Traffic in the NAT page.
2. Using the field descriptions below, specify how the router will apply the NAT rule to incoming traffic.
3. Click Create.

Priority

- Numeric value that indicates which NAT rule takes precedence if you specify more than one NAT rule for an IP address.
- Value—Integer in the range specified by the online help for this field
- Guidelines—You must specify a priority for the NAT rule. A lower number indicates a higher priority. Use a unique priority for each NAT rule that relates to the same traffic. If two rules have the same priority, they will be applied to traffic in an unpredictable order.

- Default—No value
- Example—5

Name

- Name of the NAT rule
- Value—Text string
- Default—No value
- Example—rule1

Public IP

- Public IP address that the router translates to a private address in the enterprise.
- Value—IP address
- Guidelines—Select the public destination address that is to be translated into a private destination address inside the enterprise.
- Default—No value

Private IP

- Private IP address to which the router translates the public IP address.
- Value—IP address
- Guidelines—Enter the private address of the host you wish to make available outside the enterprise.
- Default—No value

Application

- Application object to which the router will apply NAT.
- Value
  - <application>—An application object that you created (see *Classifying Traffic for Stateful Firewall Exceptions and NAT Rules* on page 491)
  - Any—Any application
- Guidelines—Select a value from the menu.
- Default—Any
- Example—myVideoConference

Enabled

- Whether or not the router applies NAT to incoming traffic on this access.
- Value
  - Enabled—Checked box
  - Disabled—White box
- Default—Disabled

Configuring Fixed Public Addresses for Outgoing Traffic

To configure fixed public IP addresses for outgoing traffic:

1. Set the portal configuration level to Advanced (see *Setting the Configuration Level for Enterprise Manager Portal* on page 466).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the NAT page (see Figure 43 on page 517).
3. Click **Create**.

Modifying NAT Rules

To modify a NAT rule:

1. Modify the entry in the appropriate table.
2. Click **Apply**.

Deleting NAT Rules

To delete a public IP address for outgoing traffic, click delete for the address range in the Public Addresses for Outgoing Traffic table.

Monitoring the Status of Subscriptions

To monitor the status of a subscription:

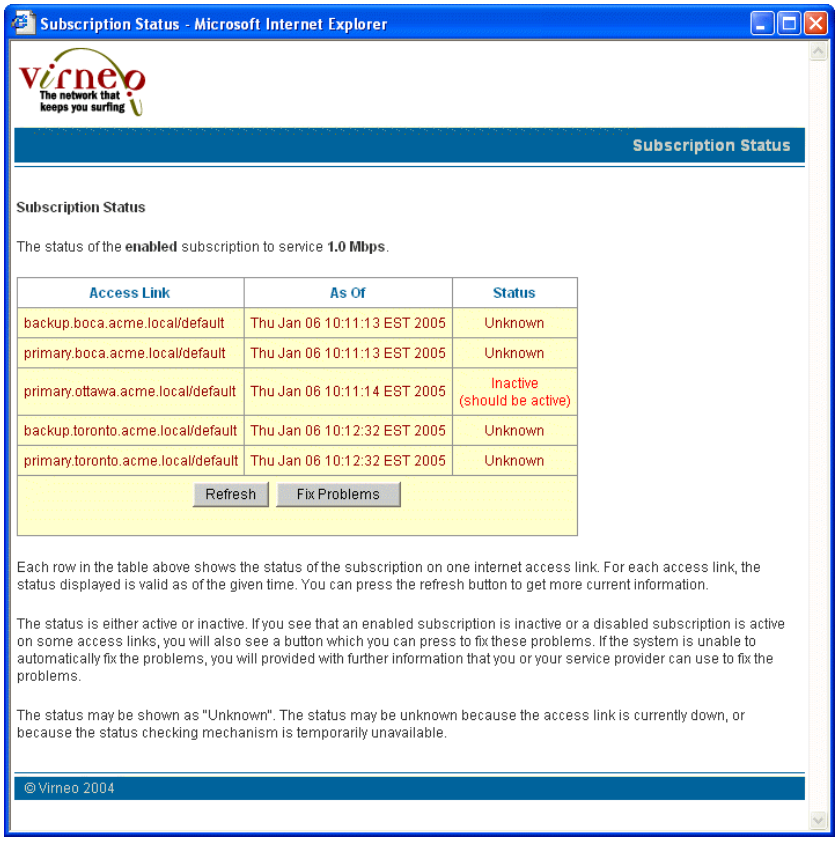
1. Start at the page that lists information about the subscription.

   For an example, see Figure 35 on page 477, which shows BoD subscriptions.
2. In the last cell of the row of data for the subscription, click **Status**.

   The Subscription Status page appears.

The Subscription Status page displays the status of this subscription for all accesses subordinate to this subscriber. The page appearance varies depending on whether the subscription is scheduled. You can click the Refresh button to update status information.

The following Subscription Status page shows the status for an unscheduled subscription.



The following Subscription Status page shows the status for a scheduled subscription.

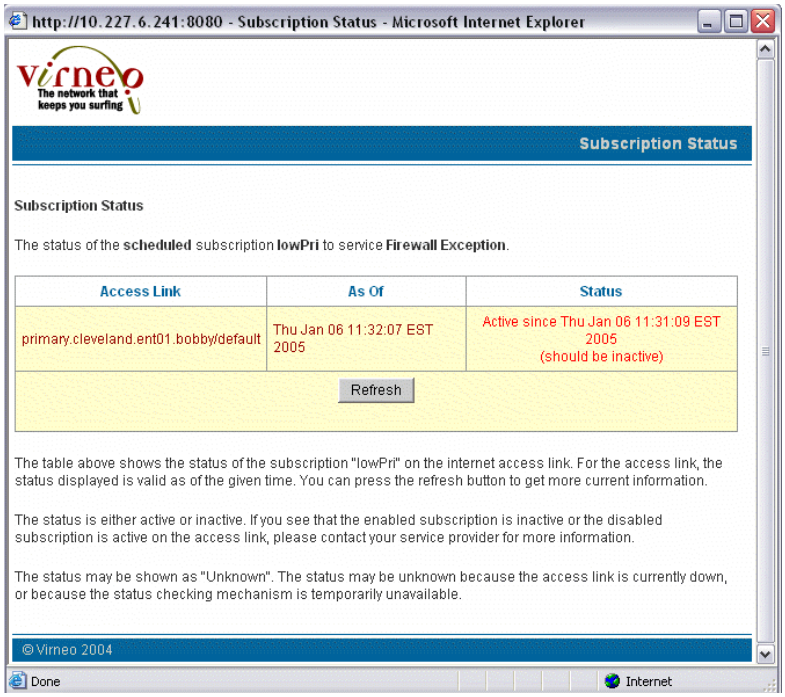


Table 43 shows the possible status for subscriptions.

Table 43: Statuses of Subscriptions

Status	Meaning	Category
Active	Subscription is enabled and is operative.	Subscription is functioning correctly.
Inactive	Subscription is disabled.	Subscription is functioning correctly.
Active (should be inactive)	Subscription is disabled but is operative.	Subscription is not functioning correctly.
Inactive (should be active)	Subscription is enabled but is inoperative.	Subscription is not functioning correctly.
Unknown	Enterprise manager Portal cannot currently communicate with the SAE, typically because the access is not functioning correctly or the checking mechanism is temporarily unavailable.	Subscription may be functioning correctly, but another problem exists.

Troubleshooting Subscriptions That Are Not Functioning Correctly

If one or more subscriptions are not functioning correctly, the Fix Problems link appears in the Subscription Status page. To troubleshoot the problems with the nonfunctioning subscriptions, click **Fix Problems**. This action causes Enterprise Manager Portal to attempt to resolve the problems with the subscriptions.

If Enterprise Manager Portal succeeds in resolving the problems, the Subscription Status page displays the new settings. Otherwise, the Subscription Status page displays more information about the problems.

Troubleshooting Subscriptions of Unknown Status

If subscriptions of unknown status and subscriptions that are not functioning correctly exist, the software will also attempt to update the unknown subscriptions when you click Fix Problems. If Enterprise Manager Portal cannot resolve the status, it will remain unknown.

If you have subscriptions of unknown status and either the Fix Problems link is not available or using the link does not resolve the status, click **Subscription Status** page. If this action does not solve the problem, check the status of the subscription later.