

Chapter 5

Using EASPs

This chapter describes how IT managers and service providers can use EASPs to log into the SDX network and to manage subscribers, services, and subscriptions in their enterprises. The chapter contains the following sections:

Configuring Your Web Browser on page 73

Accessing EASPs on page 73

Displaying Information About Your Control in the Enterprise on page 74

Updating Data That the EASP Displays on page 75

Managing Operators on page 75

Using the Demo EASP on page 77

Using the Enterprise Manager Portal on page 84

Using the NAT Address Manager Portal on page 106

For information about the EASP IT manager audit plug-in, see *Chapter 6, EASP IT Manager Audit Plug-In*.

Configuring Your Web Browser

Before you can use an EASP, you must enable your Web browser to:

Allow cookies from the EASP.

(Enterprise Manager and NAT Address Manager portals only) Use JavaScript.

Accessing EASPs

When viewing the EASPs, take care to open only one browser window yourself. The EASPs automatically open pop-up windows for various operations. If you open more than one browser window yourself, The information in the original window may not be updated correctly when you complete an operation in a pop-up window.

To access an EASP:

1. Enter the URL of the portal in your Web browser, and press Enter. For example, to access the Enterprise Manager portal, type:

```
http://192.0.2.1:8080/entmgr
```

The EASP displays the login page.

2. Select your service provider from the Retailer menu.
3. Enter your username in the Login ID field and your password in the Password field.

The EASP displays your welcome page. On the left of the page is a navigation tree for the objects in the service provider's directory over which you have control. Your login identity is the root of this navigation tree.

Displaying Information About Your Control in the Enterprise

To display information about your scope of control and permissions in the Enterprise, click the icon for the operator at the root of the navigation tree. The portal displays your welcome page.

The screenshot shows the Virneo Enterprise Portal interface. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". The top right corner displays "Virneo Enterprise Portal" and a "Log out" button. Below the header, there is a "Navigation" menu on the left and a "Welcome ent-admin" message on the right. The navigation tree includes a root node "ent-admin" (with a person icon) and several sub-nodes: "default", "retailer-one", "retailer-two", "SP", and "virtual-SP". A "Refresh" button is located below the navigation tree. The main content area displays the following information:

Please click on the tree to the left to view or modify the enterprises, sites, accesses, services, and managers under your control.

You are currently logged in as:
ent-admin

Your scope of control is:

Retailer:	all
Retailer Folders:	all
Enterprise:	all
Enterprise Folders:	all
Site:	all
Site Folders:	all
Access:	all

You have the following privileges:

Administrator:	true
Activate subscriptions:	false
Modify subscriptions:	false
Modify substitutions:	false

At the bottom left of the page, the copyright notice reads "© Juniper Networks 2003-2004".

Updating Data That the EASP Displays

To update the data that the EASP displays, click Refresh in the navigation tree. This action deletes data from the EASP cache and causes the EASP to display new data from the directory. If you refresh a Web page in the portal with the Web browser's refresh utility, the Web browser displays data from the cache, and you may not see the latest data.

Managing Operators

Normally, the service provider uses an LDAP client or SDX Admin to create one operator for each enterprise. This operator represents the primary IT manager for the enterprise (see *SDX Objects Guide*, Chapter 2, *Managing Subscriber s and Subscriptions*). The primary IT manager uses the EASP to create other operators in the directory and gives those operators privileges to manage specific sites and accesses. This section describes how IT managers can manage operators with the EASPs we provide.

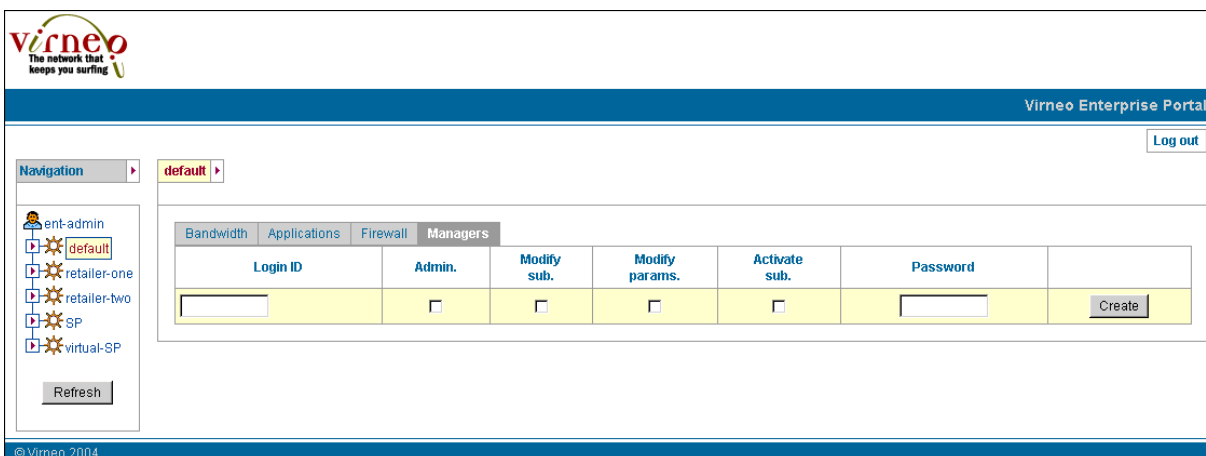
Creating Operators

To create operators through the EASP:

1. In the navigation tree of the EASP, click the object that you want to the operator to manage.
2. Click the Managers tab in the portal.

The portal displays the Manager's page for the object.

Figure 3: Manager's page



3. Complete the fields in a new line of the table, and click Create.

The portal adds the new operator to the table.

Login ID

Specifies the name that this operator uses to access the enterprise portal.

Value – text string

Guidelines – Login IDs for enterprises must be unique within the whole enterprise; retailer-level login IDs must be unique to the retailer.

Default – unspecified

Example – operator1

Admin.

Specifies whether the operator has complete control over operators, subscribers, subscriptions, substitutions, and subscription sessions for this object and its subordinate objects.

Value – Enabled | Disabled

Enabled – checked box

Disabled – white box

Default – disabled

Modify Sub.

Specifies whether the operator has complete control over subscriptions and subscription sessions for this object and its subordinate objects.

Value – Enabled | Disabled

Enabled – checked box

Disabled – white box

Default – disabled

Modify params.

Specifies whether the operator can manage substitutions in subscribers and subscriptions for this object and its subordinate objects.

Value – Enabled | Disabled

Enabled – checked box

Disabled – white box

Default – disabled

Activate sub.

Specifies whether the operator can configure automatic activation of subscriptions and manually activate and deactivate subscription sessions for this object and its subordinate objects.

Value – Enabled | Disabled

Enabled – checked box

Disabled – white box

Default – disabled

Password

Specifies the password that this operator uses to access the enterprise portal.

Value – text string

Default – unspecified

Example – secret

Modifying Operators

To modify an operator's privileges:

1. Start at the Manager's page (see Figure 3 on page 75).
2. Change the values in the fields for this operator.
3. If you want to revert to the original values, click Reset.
4. Click Apply.

Deleting Operators

To delete an operator:

1. Start at the Manager's page (see Figure 3 on page 75).
2. Click Delete for the operator.

Using the Demo EASP

The Demo EASP is a sample portal that illustrates how service providers can make their services available to IT managers in an enterprise and provides developers with a starting point from which they can create their own EASPs. This section describes how the IT managers can use this EASP.

Subscribing to Services

To subscribe to a service:

1. In the navigation tree, click the subscriber for whom you want to create a subscription to a service.

The portal displays the information for that subscriber.

2. Click the Services tab.

The Services page appears and displays the list of services available to this subscriber and the subscriber's current subscriptions.

The screenshot shows the Virneo Enterprise Portal interface. The navigation tree on the left includes 'ent-admin', 'default', 'local', 'Acme', 'Boca', 'Backup', 'Primary', 'Ottawa', 'Toronto', 'retailer-one', 'retailer-two', 'SP', and 'virtual-SP'. The main content area displays a table with the following columns: Service, Current local subscriptions, and New local subscription name. The table lists various services with their current local subscriptions and a 'Subscribe' button for each.

Service	Current local subscriptions	New local subscription name	
Internet-Gold	[unnamed]	<input type="text"/>	Subscribe
News		<input type="text"/>	Subscribe
Video-Bronze	video-bronze-boca-primary1	<input type="text"/>	Subscribe
Audio-Bronze		<input type="text"/>	Subscribe
PingDoSPProtect		<input type="text"/>	Subscribe
StaticDestNat		<input type="text"/>	Subscribe
MultiService		<input type="text"/>	Subscribe
DynSrcNat		<input type="text"/>	Subscribe
GoldSecured		<input type="text"/>	Subscribe
Internet-Silver		<input type="text"/>	Subscribe
ISP-SP		<input type="text"/>	Subscribe
Video-Silver		<input type="text"/>	Subscribe
Audio-Silver		<input type="text"/>	Subscribe
Video-Gold		<input type="text"/>	Subscribe
Silver		<input type="text"/>	Subscribe
BrickWall		<input type="text"/>	Subscribe
GoldMetered		gold-metered-eng	Subscribe

- In the New local subscription name field, enter a name for the subscription to the service.

You can have one unnamed subscription to a service; if you have multiple subscriptions to a service, only one can be unnamed.

- Click Subscribe.

Activating Subscriptions

To activate a subscription:

- In the navigation tree, click the subscriber for whom the subscription is configured.
- Click the Subscriptions tab.

The Subscriptions page appears.

Figure 4: Subscriptions page

The screenshot shows the Virneo Enterprise Portal interface. At the top left is the Virneo logo with the tagline "The network that keeps you surfing". The page title is "Virneo Enterprise Portal" and there is a "Log out" button. A navigation pane on the left shows a tree structure with "ent-admin" at the top, followed by "default", "local", "ABCInc", "Boca", "Primary", "Backup", "Boston", "Montreal", "Ottawa", "PrimaryAccess", "Acme", "retailer-one", "retailer-two", "SP", and "virtual-SP". The "Primary" item is selected. The main content area has tabs for "Services", "Subscriptions", "Sessions", "Departments", and "Managers". The "Subscriptions" tab is active, showing a table with the following data:

Service	Subscription
BronzeMetered	[unnamed] (From site Boca)
GoldMetered	[unnamed] (From enterprise ABCInc)
PingDoSPProtect	[unnamed] (From enterprise ABCInc)

To the right of the table is the "Subscription details" section, which includes:

- Subscription Status:** Administratively inactive. (Buttons: Activate, Deactivate)
- Not suspended.** (Buttons: Unsuspend, Suspend)
- Usage:** (Button: Reporting)
- Service Parameters:** (use checkbox to lock value). dept = acct (From subscription in enterprise ABCInc). (Buttons: Apply, Delete, Reset)
- Action:** (Button: Unsubscribe)

At the bottom left of the page, there is a "Refresh" button and a copyright notice: "© Juniper Networks 2003-2004".

3. In the Subscription column, click the subscription that you want to activate.
4. In the Subscription details area, click Activate.

Deactivating Subscriptions

To deactivate a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 4).
2. In the Subscription column, click the subscription you want to deactivate.
3. Click Deactivate.

Suspending Subscriptions

You can prevent a subscriber from inheriting a subscription by suspending that subscription. To do so:

1. Start at the subscriber's Subscriptions page (see Figure 4).
2. In the Subscription column, click the subscription you want to suspend.
3. Click Suspend.

Canceling Suspensions of Subscriptions

If you suspend a subscription for a subscriber, you can restore the inherited subscription for that subscriber. You can also maintain the suspension for that subscriber and restore the inherited subscription for that subscriber's subordinate subscribers. To do so:

1. Start at the Subscriptions page (see Figure 4) for the subscriber for which you want to restore the inherited subscription.
2. In the Subscription column, click the subscription you want to allow.
3. Click Unsuspend.

Monitoring Use of Subscriptions

To monitor the use of a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 4).
2. In the Subscription column, click the subscription you want to view.
3. Click Reporting.

The Usage Reporting page appears. If the EASP cannot contact the relevant SAE to obtain data for this subscriber, the page will display the statistics as Unknown.

EmailAndWeb%EmailAndWeb1 Service Session under	Usage Information					
	In Bytes	Out Bytes	In Packets	Out Packets	Update Time	Start Time
Primary.Boca.Acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown
<input type="button" value="Reload"/>						

To update the data on this page, click Reload.

Specifying Values for Service Parameters in Subscriptions

The Service Parameters column lists the parameters you can specify for this subscription. Subscriptions inherit values for service parameters from subscriptions of parent subscribers. If the parameter is locked by the parent subscriber, the value is gray in the portal and you cannot modify the value. If the parameter is not locked by a parent subscriber, you can modify the value.

To specify a value for a parameter:

1. Start at the subscriber's Subscriptions page (see Figure 4 on page 79).
2. Locate the parameter in the Service Parameters column.
3. Provide a value for this parameter.
4. (Optional) Select Locked to prevent operators of subordinate subscribers from changing this value.

5. If you want to revert to the original values, click Reset.
6. Click Apply.

Restoring Default Values for Service Parameters In Subscriptions

To restore the default value for a service parameter:

1. Start at the subscriber's Subscriptions page (see Figure 4 on page 79).
2. Locate the parameter in the Service Parameters column.
3. Click Delete.

Some services may have parameters without a default value. If you do not supply values for these parameters, the SAE cannot perform the substitutions when it tries to activate a service, and the activation will fail.

Deleting Subscriptions

To delete a subscription:

1. Start at the subscriber's Subscriptions page (see Figure 4 on page 79).
2. Click the subscription you want to delete.
3. Click Unsubscribe.

Monitoring Service Sessions for a Subscription

To monitor the service sessions for a subscription:

1. In the navigation tree, click the access for which you want to monitor the sessions.

The portal displays the information for that access.

2. Click the Sessions tab.

The portal displays the status of each subscription and the parameters associated with each service subscription.

The screenshot shows the Virneo Enterprise Portal interface. On the left is a navigation tree with a 'Refresh' button. The main content area shows a breadcrumb trail: default > local > ABCInc > Boca > Primary. Below this are tabs for Services, Subscriptions, Sessions, Departments, and Managers. The 'Departments' tab is active, displaying a table with the following data:

Service Name	Oper Active	Service Parameter		
		Name	Admin Value	Op Value
PingDoSPProtect	unknown	dept	0.0.0.0/0	Unknown
GoldMetered	unknown	dept	208.93.36.64/28	Unknown
BronzeMetered	unknown	dept	208.93.36.80/28	Unknown

A 'Reload' button is located at the bottom of the table.

To update the data on this page, click Reload.

Defining Networks for Departments in an Enterprise

To define the networks for departments in an enterprise:

1. In the navigation tree, click the subscriber for whom you want to define the department.

The portal displays the information for that subscriber.

2. Click the Departments tab.

The Departments page appears.

Figure 5: Departments page

The screenshot shows the Virneo Enterprise Portal interface. On the left is a navigation tree with a 'Refresh' button. The main content area has a breadcrumb trail: default > local > Acme > Boca > Primary. Below the breadcrumb is a tabbed interface with 'Departments' selected. The table below has the following data:

Department	Department network	Locked	
eng	192.0.2.22/2	<input checked="" type="checkbox"/>	Apply Delete Reset
acct	192.0.2.22/3	<input type="checkbox"/>	Apply Delete Reset
		<input type="checkbox"/>	Create

© Juniper Networks 2003-2004

3. In the Department field, enter the name of the department.
4. In the Department network field, enter the network that this department uses, or leave this field empty to use the department name.
5. (Optional) Select Locked to prevent operators of subordinate subscribers from changing this value.
6. Click Create.

This feature illustrates how service providers can use parameters and substitutions in the portal. The fields called Department and Department network are a name and value for a substitution respectively. These parameters are also defined in SDX objects such as services and policies. The IT manager provides actual values for the parameters through the portal. Service providers could use these parameters to track and charge each department for the volume of bandwidth it uses. For more information about parameters and substitutions, see *SDX Objects Guide, Chapter 6, Parameter Value Acquisition (JUNOS Routers)* and *SDX Objects Guide, Chapter 9, Parameter Value Acquisition (JUNOS Routing Platforms)*.

Modifying Network Definitions for Departments in an Enterprise

To delete a network definition for a department:

1. Start at the subscriber's Departments page (see Figure 5).
2. Modify values for the department.
3. If you want to revert to the original values, click Reset.
4. Click Apply.

Deleting Network Definitions for Departments in an Enterprise

To delete a network definition for a department:

1. Start at the subscriber's Departments page (see Figure 5).
2. Click Delete for the department.

Using the Enterprise Manager Portal

IT managers who connect to the SDX network through a JUNOS routing platform use the Enterprise Manager portal to activate services, subscribers, and subscriptions for that enterprise. The services that the IT managers can use depend on those that the service provider offers (see *Chapter 4, Installing and Configuring EASPs*). If you offer 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 the 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 the Enterprise Manager Portal

The default setting for the configuration level is Normal. With this setting you can configure most services on the 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 tree.

The operator's welcome page appears.



Virneo Enterprise Portal

[Log out](#)

Navigation > Welcome ent-admin >

ent-admin

- default
- retailer-one
- retailer-two
- SP
- virtual-SP

Refresh

Please click on the tree to the left to view or modify the enterprises, sites, accesses, services, and managers under your control.

You are currently logged in as:
ent-admin

Your scope of control is:

Retailer:	all
Retailer Folders:	all
Enterprise:	all
Enterprise Folders:	all
Site:	all
Site Folders:	all
Access:	all

You have the following privileges:

Administrator:	true
Activate subscriptions:	false
Modify subscriptions:	false
Modify substitutions:	false

Portal mode:
Normal

© Virneo 2004

2. Select Advanced from the Portal mode menu.

Subscribing to Bandwidth on Demand (BoD) Services

The service provider makes BoD services available to enterprises. You can specify the traffic in the enterprise for which you want to enable BoD subscriptions. Subordinate subscribers inherit BoD subscriptions configured for parent subscribers. To create a subscription to a BoD service:

1. In the navigation tree of the EASP, click the subscriber for which you want to provision BoD.
2. Click the BoD tab.

The Bandwidth page appears. This page displays BoD subscriptions that the subscriber inherits from parent subscribers and BoD subscriptions configured explicitly for the subscriber.

Figure 6: Bandwidth page

The screenshot shows the Virneo Enterprise Portal interface. On the left is a navigation tree with a 'Refresh' button. The main content area is titled 'Bandwidth' and contains a table with the following structure:

Name	Service	IP Protocol	TOS Byte	Source IPs & Ports	Destination IPs & Ports	Enabled	
BoD1	Gold	gre		192.0.2.1/22	192.0.2.22/22	<input checked="" type="checkbox"/>	Inherited from site "Boca". Show usage data...
RSVPbod	Gold	rsvp		192.0.2.23/22	192.0.2.40/22	<input type="checkbox"/>	Inherited from enterprise "Acme". Show usage data...
tcpBoD	Gold	tcp	8/255	192.0.2.1/23 1.22.25	192.0.2.22/23 2.26.29	<input checked="" type="checkbox"/>	Apply Delete Show usage data...
	Gold					<input type="checkbox"/>	Create

- Using the field descriptions below, configure the values for this subscriber's bandwidth.
- Click Create.

Name

Specifies name of the subscription to the BoD service.

Value – text string

Default – unspecified

Example – lowBandwidth

Service

Specifies name of the BoD service in the directory that will be applied to the subscription.

Value – menu of BoD services available for this subscriber

Default – BoD service with lowest alphanumeric name in the directory

Example – BoD2

IP Protocol

Specifies the IP protocol associated with traffic affected by this bandwidth rule.

Value – ah | egp | esp | gre | icmp | igmp | ipip | ipv6 | ospf | pim | rsvp | sctp | tcp | udp | < 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.

Default – unspecified

Example – tcp

TOS Byte

Specifies the type of service (ToS) byte and mask in the header of the IP datagram.

Value – < tosByte> /< tosMask>

Guidelines – The portal displays this feature only if you select the configuration level Advanced (see *Setting the Configuration Level for the Enterprise Manager Portal on page 84*). Specify the ToS byte and mask in this field if you want to enable BoD for a specific ToS. If you want to enable BoD for all types of service, leave this field empty.

Default – unspecified

Example – 8/25

Source IP Address

Specifies the source IP addresses (as contained in the IP packets) of traffic for which BoD will be enabled.

Value – [not]< networkAddress> /< networkMask>

not – specifies 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 in the upper field. 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 upper field empty.

To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for the Enterprise Manager Portal on page 84*), and enter multiple addresses on different lines. The order in which you list prefixes 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.

Default – unspecified; default subnet mask is 32

Example – in this example, 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

Specifies the source TCP/UDP ports (as contained in the IP packets) of traffic for which BoD will be enabled.

Value – comma-separated list of port numbers and ranges of port numbers; ranges of port numbers are separated by two dots (..).

Guidelines – To specify particular source TCP/UDP ports, specify the port numbers in the lower field. To specify all ports, leave this field empty.

Default – unspecified

Example – 2, 3, 45..55

Destination IP Address

Specifies the destination TCP/UDP ports (as contained in the IP packets) of traffic for which BoD will be enabled.

Value – [not]< networkAddress> /< networkMask>

not – specifies 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 in the upper field. 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 the Enterprise Manager Portal on page 84*), and enter multiple addresses on different lines.

Default – unspecified

Example – 192.0.2.0/24

Destination Ports

Specifies the destination TCP/UDP ports (as contained in the IP packets) of traffic for which BoD will be enabled.

Value – comma-separated list of port numbers and ranges of port numbers; ranges of port numbers are separated by two dots (..).

Guidelines – To specify particular TCP/UDP ports, specify the port numbers in the lower field. To specify all ports, leave this field empty.

Default – unspecified

Example – 2, 3, 45..55

Enabled

Specifies status of the subscription.

Value – gray box | white box | box with check mark | empty box

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 BoD Subscriptions

To modify a BoD subscription:

1. Start at the subscriber's Bandwidth page (see Figure 6 on page 86).
2. Change the values in the fields for this subscription.
3. Click Apply for the subscription.

Deleting BoD Subscriptions

To delete a BoD subscription:

1. Start at the subscriber's Bandwidth page (see Figure 6 on page 86).
2. Click Delete for the subscription.

Monitoring Use of BoD Subscriptions

To monitor the use of a BoD subscription:

1. Start at the subscriber's Bandwidth page (see Figure 6 on page 86).
2. Click Show Usage data for the subscription.

The Bandwidth-on-Demand Usage page appears.

Bandwidth-on-Demand Usage

Bandwidth-on-Demand Usage Data

This data is for subscription **BoD1** to service **Gold**.

Access Link	Usage Data					
	For Period From	For Period To	Incoming Bytes	Outgoing Bytes	Incoming Packets	Outgoing Packets
Backup.Boca.Acme.local/default	Unknown	Unknown	Unknown	Unknown	Unknown	Unknown

Each row in the table above shows usage data for the subscription "BoD1" on one internet access link. For each access link, the usage data covers the period starting when the service was most recently activated on that access link, and ending when the usage data was most recently collected from the network infrastructure. Usage data is collected periodically (e.g. once an hour).

Usage data may be shown as "Unknown". Usage data may be unknown because no data has yet been collected for a particular access link, or because the access link is currently down, or because the usage data collection mechanism is temporarily unavailable.

© Virneo 2004

Creating Application Objects

You can create for a subscriber a list of application objects that can be used to classify the traffic affected by a firewall exception or 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.

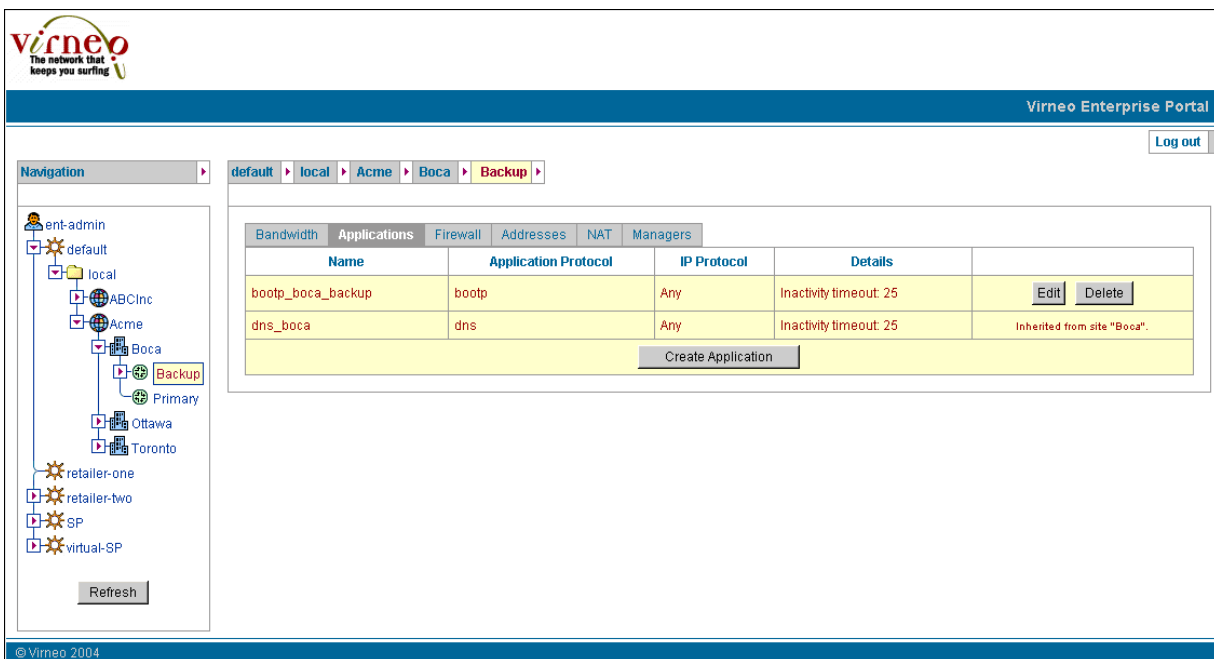
Certain application protocols, such as FTP, are supported explicitly and you can select them for your application object. These application protocols usually have an associated IP protocol that the portal selects automatically. If you want to create an application object for application protocol that 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.

To create an application protocol:

1. Click the subscriber to which you want to assign the application protocol.
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 7: Applications page



The screenshot shows the Virneo Enterprise Portal interface. The top navigation bar includes the Virneo logo and the text "Virneo Enterprise Portal". A "Log out" button is located in the top right corner. The main content area is divided into a navigation pane on the left and a main content area on the right. The navigation pane shows a tree structure with nodes for "ent-admin", "default", "local", "ABCInc", "Acme", "Boca", "Backup", "Primary", "Ottawa", "Toronto", "retailer-one", "retailer-two", "SP", and "virtual-SP". The "Backup" node is highlighted. The main content area shows a breadcrumb trail: "default > local > Acme > Boca > Backup". Below the breadcrumb trail are tabs for "Bandwidth", "Applications", "Firewall", "Addresses", "NAT", and "Managers". The "Applications" tab is selected. A table displays the application protocols for the selected subscriber:

Name	Application Protocol	IP Protocol	Details	
bootp_boca_backup	bootp	Any	Inactivity timeout: 25	Edit Delete
dns_boca	dns	Any	Inactivity timeout: 25	Inherited from site "Boca".

Below the table is a "Create Application" button. The footer of the page contains the text "© Virneo 2004".

3. Click Create Application.

The Create Application page appears.

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

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

- Click Apply.

Application Name

Specifies a name for this application protocol.

Value – text string

Default – unspecified

Example – bootp-boston

Application Protocol

Specifies the application protocol.

Value – type of application protocol | 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 conversation. Consequently, you can deny or discard a conversation, but you cannot allow a complete conversation.

Default – Any

Example – bootp

IP Protocol

Specifies the IP protocol.

Value – type of IP protocol | 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 – unspecified

Example – tcp

Source Port

Specifies the 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 – unspecified

Example – 25..35

Destination Port

Specifies the 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 – unspecified

Example – 25..35

SNMP Command

Specifies the type of command for SNMP.

Value – type of SNMP command

Guidelines – Select a type of command from the menu.

Default – Any

Example – get-next

ICMP Type

Specifies the type of message for ICMP.

Value – type of ICMP message

Guidelines – Select a type of message from the menu.

Default – Any

Example – info-reply

ICMP Code

Specifies the 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

Specifies the depth of network penetration for the traceroute application protocol.

Value – integer in the range 0–255 | unspecified

unspecified – allows traceroutes up to a depth of 255.

Default – unspecified

Example – 5

RPC Program Number

Specifies the program number for the RPC application protocol.

Value – a single program number or range of program numbers separated by two dots (.). Program numbers are integers in the range 100,000–400,000.

Guidelines – Specify the RPC program numbers to which the NAT rule or firewall exception apply. To specify all RPC program numbers, leave this field empty.

Default – unspecified

Example – 7..12

UUID

Specifies the universal unique identifier (UUID) for the 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 – unspecified

Example – 1f356a25-ce67-73ad-2187-631ec8ae1bd6

Inactivity Timeout

Specifies the time for which a conversation associated with the specified application protocol can be inactive before the JUNOS routing platform terminates the conversation.

Value – integer in the range 0–2147483647 seconds

Guidelines – Specify a time, or leave this field empty to use the default setting.

Default – 30 seconds

Example – 45

Modifying Values for Application Objects

To modify values for an application object:

1. Start at the Applications page (see Figure 7 on page 91).
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 Application Objects

To delete an application protocol:

1. Start at the Applications page (see Figure 7 on page 91).
2. Click Delete for the application protocol.

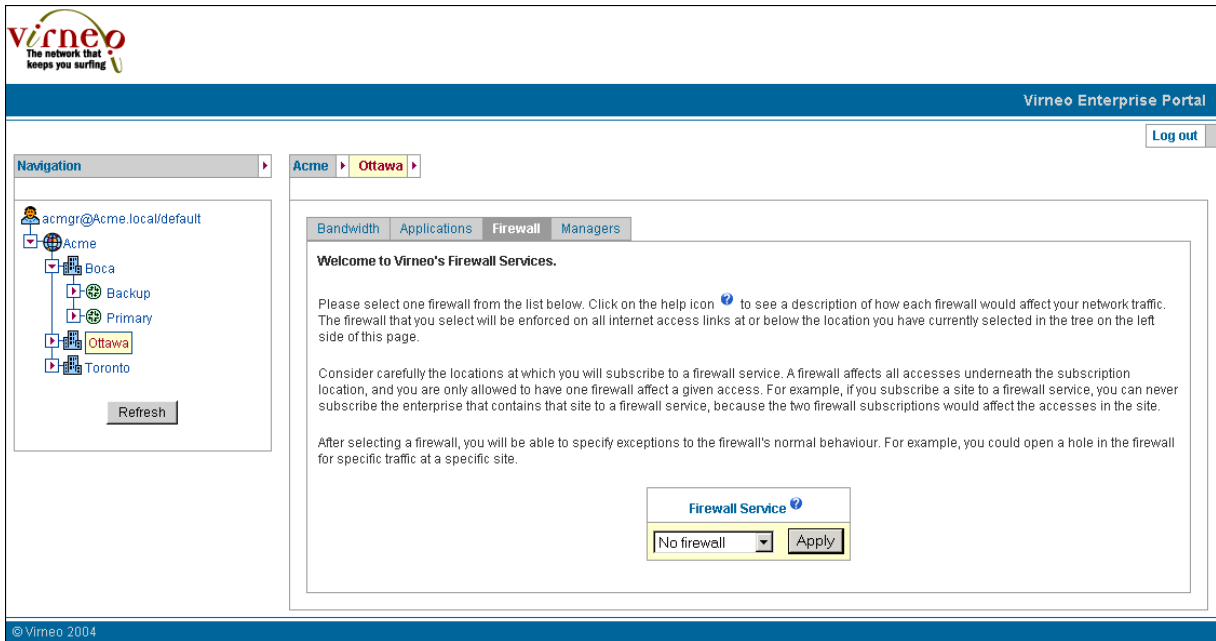
Subscribing to Firewall Services

The basic firewall that you configure will be enforced on all Internet access links subordinate to the subscriber you select in the navigation tree. When you have configured a basic firewall, you can create firewall exceptions—variances from the basic firewall—for specific categories of traffic. For example, you can create firewall exceptions for traffic associated with a particular application protocol, such as FTP, that originates at a particular address in the enterprise. See *Creating Application Objects on page 90* for information about defining an application object, which defines traffic associated with a particular application protocol.

To create a subscription to a basic firewall service:

1. In the navigation tree of the EASP, click the subscriber for which you want to create a subscription to a basic firewall service.
2. Click the Firewall tab.

The Firewall page appears.




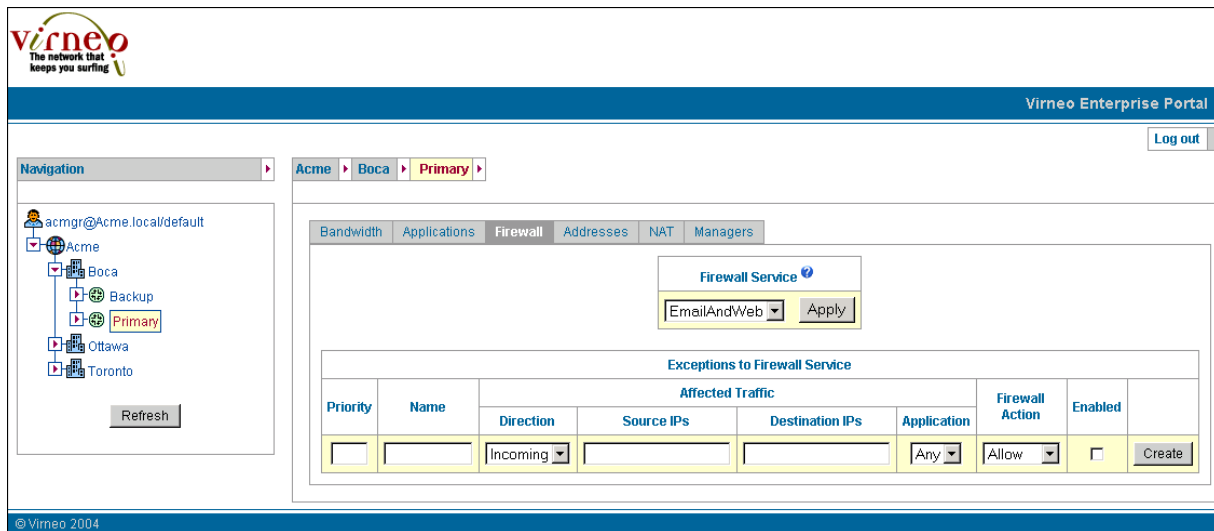
3. Click the help icon  above the firewall service to review information about the available firewalls.
 4. Select a firewall service from the menu, and click Apply.
- The Firewall page changes.

Figure 8: Firewall page



Firewall Service

Specifies the firewall service.

Value – menu of firewall services in the directory available for this subscriber.

Default – No Firewall

Example – BasicFW1

Creating Firewall Exceptions

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 *Creating Application Objects* on page 90).
1. Access the subscriber's Firewall page (see Figure 8).
2. Using the field descriptions below, configure the values for the firewall exception.
3. Click Create.

Priority

Specifies a 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 – unspecified

Example – 5

Name

Specifies the name of subscription to the firewall service.

Value – text string

Guidelines – You must specify a name for the firewall exception.

Default – unspecified

Example – videoConference

Direction

Specifies the direction, with respect to the enterprise, of the initial traffic flow in a conversation.

Value – Incoming | Outgoing | Both

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

Specifies the source IP addresses (as contained in the IP packets) of traffic to which the firewall exception applies.

Value – [not]< networkAddress> /< networkMask>

not – specifies 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 in the upper field. 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 upper field empty. To specify multiple source IP addresses, set the configuration level of the portal to Advanced (see *Setting the Configuration Level for the Enterprise Manager Portal on page 84*), and enter multiple addresses on different lines.

Default – unspecified

Example – 192.0.2.0/24

Destination IPs

Specifies the destination TCP/UDP ports (as contained in the IP packets) of traffic to which this firewall exception applies.

Value – [not]< networkAddress> /< networkMask>

not – specifies 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 in the upper field. 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 the Enterprise Manager Portal on page 84*), and enter multiple addresses on different lines.

Default – unspecified

Example – 192.0.2.0/24

Application

Specifies the application object to which the firewall applies.

Value – application object you defined

Guidelines – Select an application object from the menu. For information about specifying application object see *Creating Application Objects* on page 90.

Default – Any

Example – ftp

Firewall Action

Specifies how the firewall should handle the incoming or outgoing traffic.

Value – Allow | Reject | Discard

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 – Deny

Enabled

Specifies status of the firewall exception.

Value – gray box | white box | box with check mark | empty box

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

Modifying Firewall Exceptions

To modify a firewall exception:

1. Start at the Firewall page for the subscriber (see Figure 8 on page 96).
2. Change the values in the fields for this firewall exception.
3. 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 8 on page 96).
2. Click Delete for the firewall exception.

Deleting Basic Firewalls

To delete a basic firewall:

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

For information about these tasks, see *Deleting Firewall Exceptions* on page 99 and *Deleting NAT Rules* on page 106.

2. Delete all firewall exceptions and NAT rules that this subscriber inherits from parent subscribers.
3. Delete 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 8 on page 96).
5. Select No Firewall from the Firewall Service menu.
6. Click Apply.

Requesting Public IP Addresses for NAT Services

To request one or more IP addresses:

1. In the navigation tree of the Enterprise Manager portal, click the access to which you want to request an IP address.
2. Click the Address tab.

The Address page appears.

Figure 9: Address page

The screenshot shows the Virneo Enterprise Portal interface. The navigation tree on the left includes Acme, Boca, Backup, Ottawa, and Toronto. The main content area is titled 'Public IP Addresses' and contains a table with the following data:

Address	Used By	
165.165.165.165		<input type="checkbox"/>
165.165.165.166		<input type="checkbox"/>
165.165.165.167		<input type="checkbox"/>
165.165.165.168		<input type="checkbox"/>
165.165.165.169		<input type="checkbox"/>
165.165.165.170		<input type="checkbox"/>

Below the table is a 'Request More Public IP Addresses' form with the following fields:

Number of Addresses	Contiguous	
<input type="text" value="1"/>	<input type="checkbox"/>	<input type="button" value="Request"/>

At the bottom of the page, there is a section for 'Outstanding Requests for Public IP Addresses' which displays the message: 'No outstanding requests for public IP addresses exist.'

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.

The EASP 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, the EASP displays the public IP addresses assigned to this access and makes the addresses visible in the menus on the NAT page for that access. If a request for an IP address is outstanding for a certain period of time, the Enterprise Manager portal automatically sends a reminder to the service provider.

Number of Addresses

Specifies the number of IP addresses you want the service provider to supply.

Value – integer in the range 1–2147483647

Default – 1

Contiguous

Specifies whether requested multiple IP addresses should be sequential.

Value – checked box | empty box

checked box – IP addresses must be contiguous

empty box – IP address need not be contiguous

Default – empty box

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 Address page for the subscriber (see Figure 9).
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 gray, 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

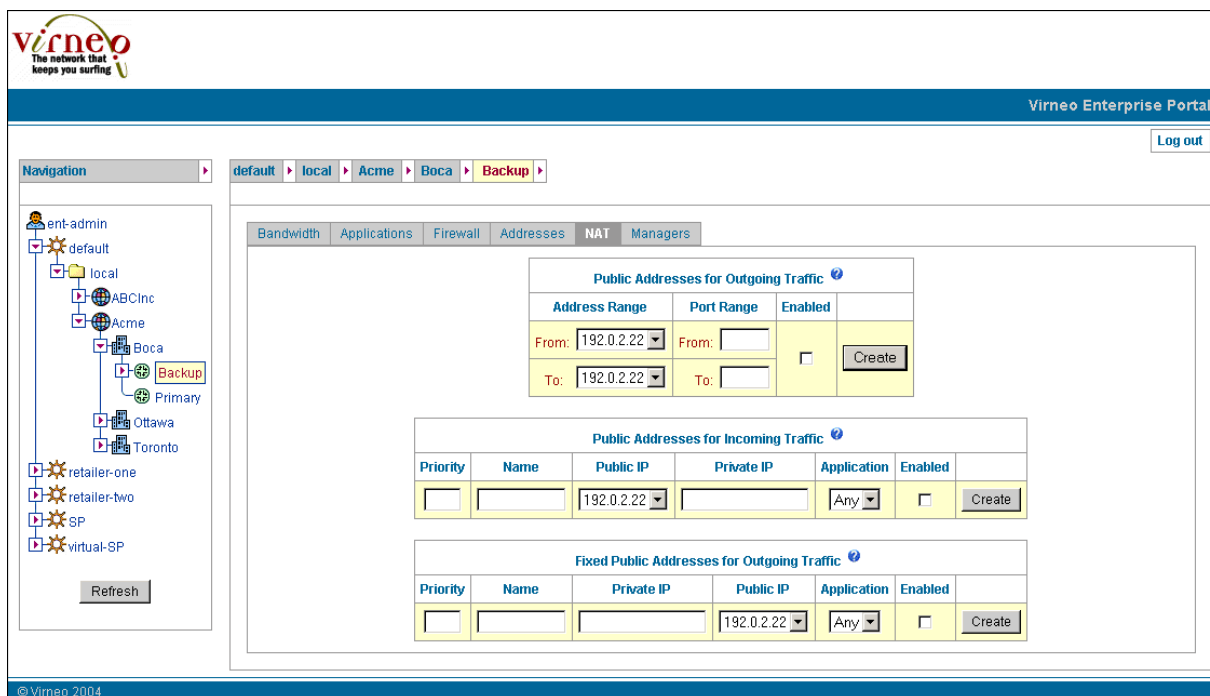
Also known as *static source NAT*, this type of NAT allows you to specify the public source IP to be used for specific outgoing traffic. To specify this type of NAT you must set the configuration level of the portal to Advanced (see *Setting the Configuration Level for the Enterprise Manager Portal* on page 84).

To apply NAT rules to traffic on JUNOS routing platforms:

1. In the navigation tree of the EASP, click the access that connects to the router.
2. Click the NAT tab.

The NAT page appears.

Figure 10: 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. Click Enabled.
4. Click Create.

Address Range

Specifies the 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 – unspecified

Port Range

Specifies the 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 – unspecified

Enabled

Specifies whether the router applies NAT to outgoing traffic on this access.

Value – Enabled | Disabled

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

Specifies a 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 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 – unspecified

Example – 5

Name

Specifies the name of the NAT rule

Value – text string

Default – unspecified

Example – rule1

Public IP

Specifies the 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 – unspecified

Private IP

Specifies the 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 – unspecified

Application

Specifies the application object to which the router will apply NAT.

Value – < application> | Any

< application> – an application object that you created (see *Creating Application Objects* on page 90)

Any – any application

Guidelines – Select a value from the menu.

Default – Any

Example – myVideoConference

Enabled

Specifies whether the router applies NAT to incoming traffic on this access.

Value – Enabled | Disabled

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 the Enterprise Manager Portal* on page 84).
2. Locate the area called Fixed Public Addresses for Outgoing Traffic in the Figure 8 on page 96.

3. Using the field descriptions below, specify how the router will apply the NAT rule to incoming traffic.
4. 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.

Using the NAT Address Manager Portal

Service providers use the NAT Address Manager portal to manage requests about public IP addresses from IT managers. When an IT manager sends a request about IP addresses through the Enterprise Manager portal, the portal sends an e-mail to the service provider that contains a link to the NAT Address Manager portal.

For demonstration purposes or for small service providers, a human administrator can deal with this e-mail manually. In a large production environment, however, the e-mail will be sent to a machine that automatically assigns addresses to accesses. For information about how a machine manages IP addresses, see *NAT Address Manager Portal* on page 47.

Assigning IP Addresses

To assign IP addresses to accesses manually:

1. Click the link to the NAT Address Manager portal in the e-mail.

The NAT Address Manager portal appears and displays the status of IP addresses for this link.

The screenshot shows the NAT Address Management interface. At the top left is the logo for 'virneo' with the tagline 'The network that keeps you surfing'. The page title is 'NAT Address Management'. Below the title is a breadcrumb trail: 'default > local > Acme > Boca > Primary >'. The main content area is divided into three sections:

- Assigned IP Addresses:** A box with the heading 'Assigned IP Addresses' and the message 'No public IP addresses have been assigned to this access link'.
- Released IP Addresses:** A box with the heading 'Released IP Addresses' and the message 'No public IP addresses have been released by this access link'.
- Outstanding Requests for Public IP Addresses:** A table with the following data:

Request Time	Number of Addresses	Must be Contiguous	
Jun 30, 2004 4:03 PM	1	false	<input type="button" value="Assign IPs"/>

At the bottom left of the interface, it says 'Copyright Juniper Networks 2004'.

2. Click Assign IPs.

The Assign Public IP Addresses window appears.

The screenshot shows the 'Assign Public IP Addresses (Contiguous)' window. It contains a table with three rows for entering IP addresses and an 'Assign' button at the bottom.

Assign Public IP Addresses (Contiguous)	
	IP Address
1	<input type="text"/>
2	<input type="text"/>
3	<input type="text"/>
<input type="button" value="Assign"/>	

3. Enter an IP address in each line of this window.
4. Click Assign.

Acknowledging the Release of IP Addresses

When an IT manager returns an IP address through the Enterprise Manager portal, the NAT Address Manager displays the returned IP address. You must acknowledge release of the IP Address to the IT manager. To do so, click Acknowledge in the Released IP Addresses table.

The screenshot displays the NAT Address Management interface. At the top left is the **virneo** logo with the tagline "The network that keeps you surfing". The top right corner shows the page title "NAT Address Management". Below the title is a breadcrumb navigation path: **default > local > Acme > Boca > Primary >**. The main content area is divided into three sections:

- Assigned IP Addresses:** A box containing the message "No public IP addresses have been assigned to this access link".
- Released IP Addresses:** A table with two columns: "Release Time" and "Released IPs". It contains one entry: "Jul 19, 2004 6:40 PM" and "192.0.2.22". Below the table is an "Acknowledge" button.
- Outstanding Requests for Public IP Addresses:** A table with three columns: "Request Time", "Number of Addresses", and "Must be Contiguous". It contains one entry: "Jul 18, 2004 2:55 PM", "1", and "false". To the right of the table is an "Assign IPs" button.

At the bottom left of the page, there is a copyright notice: "Copyright Juniper Networks 2004".