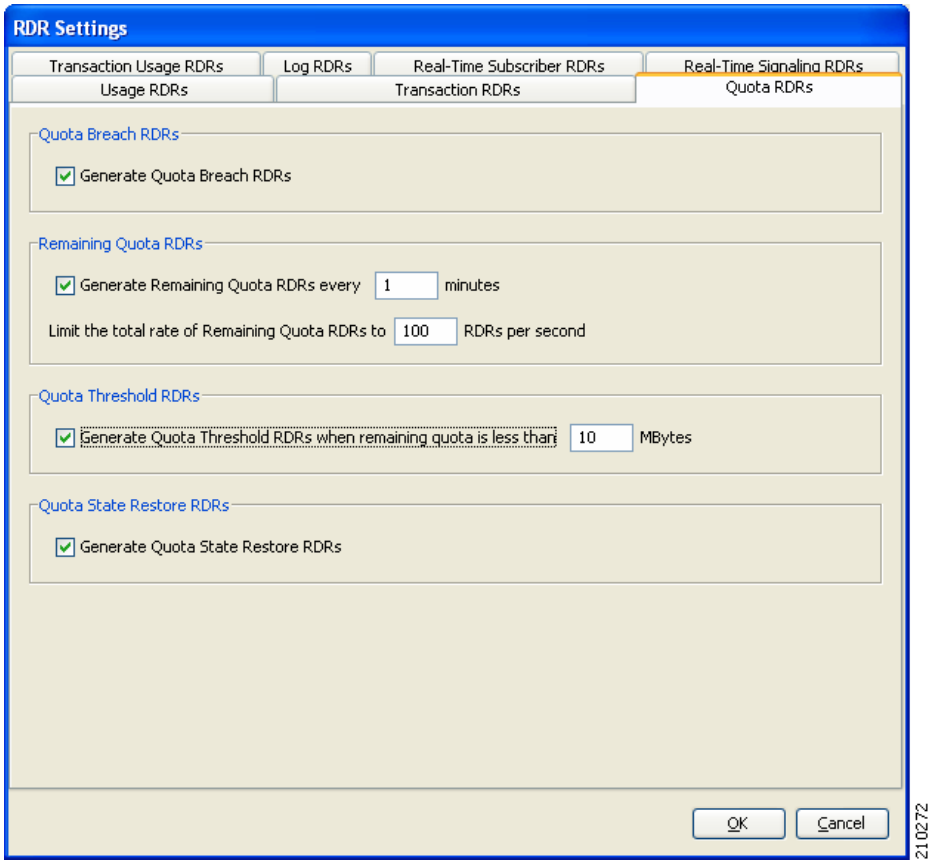
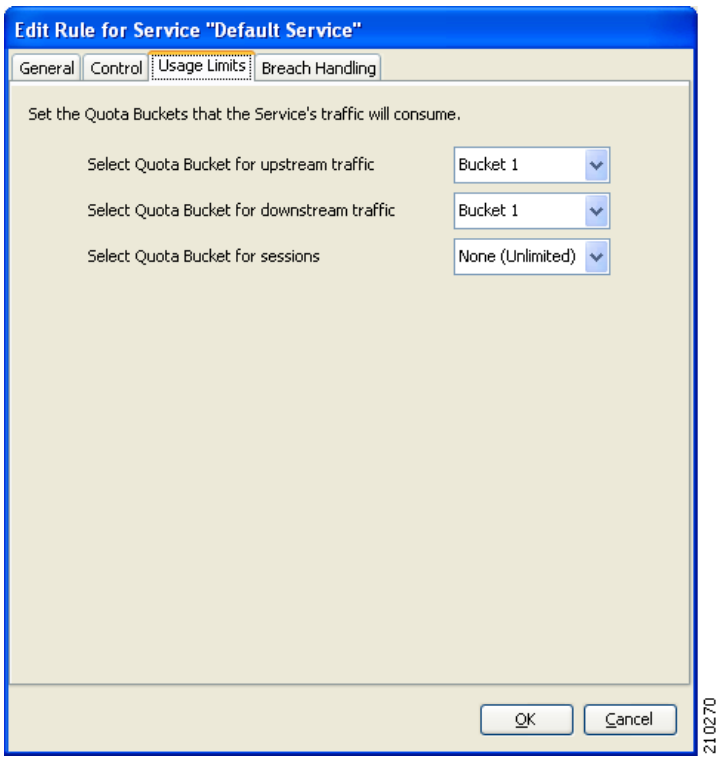
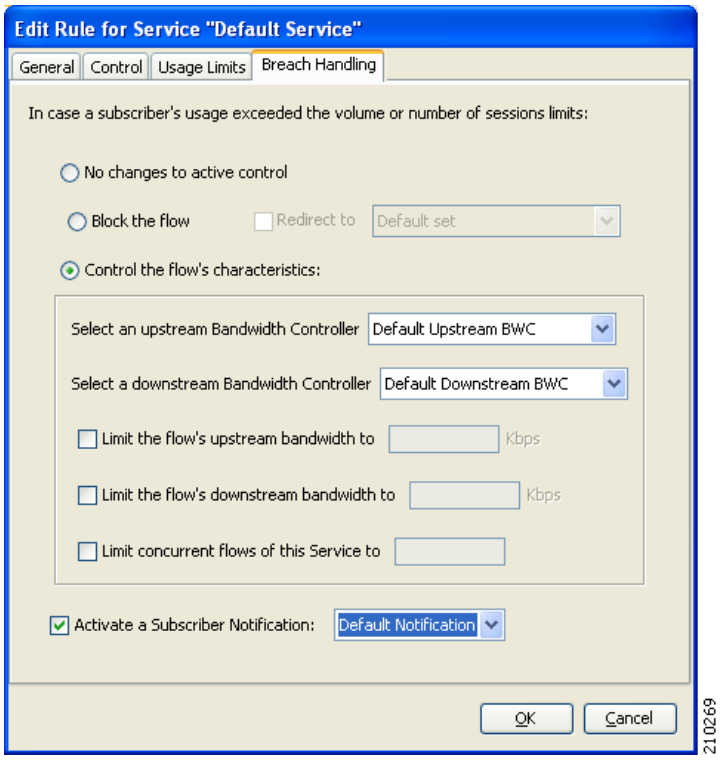
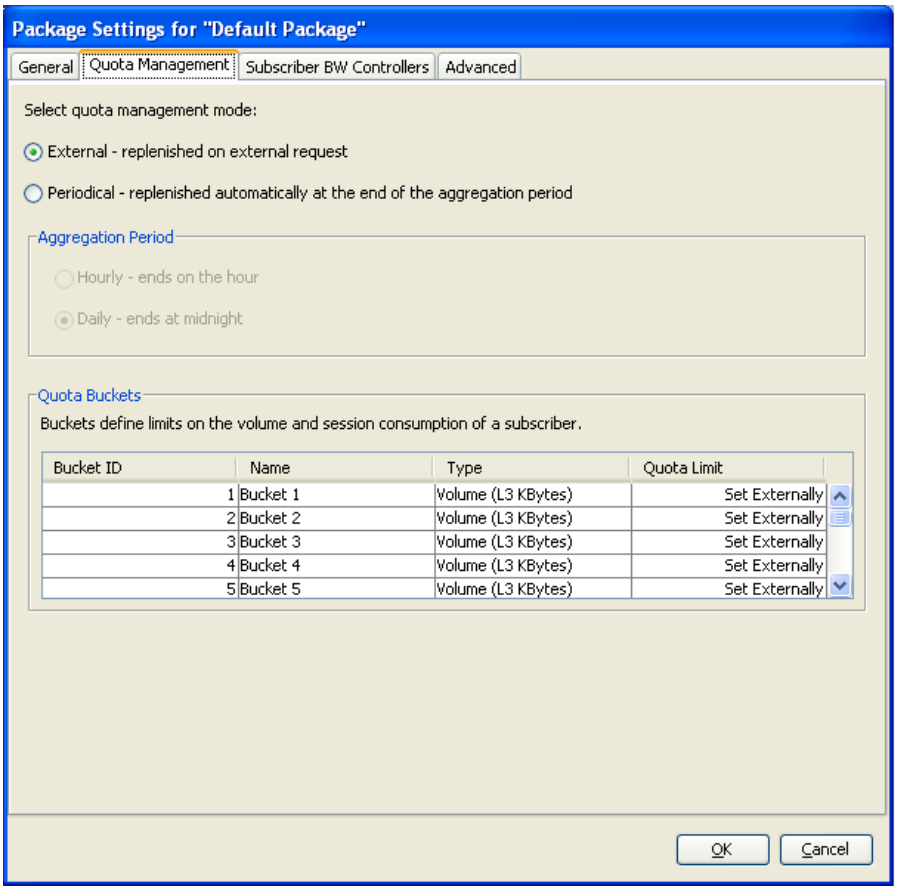
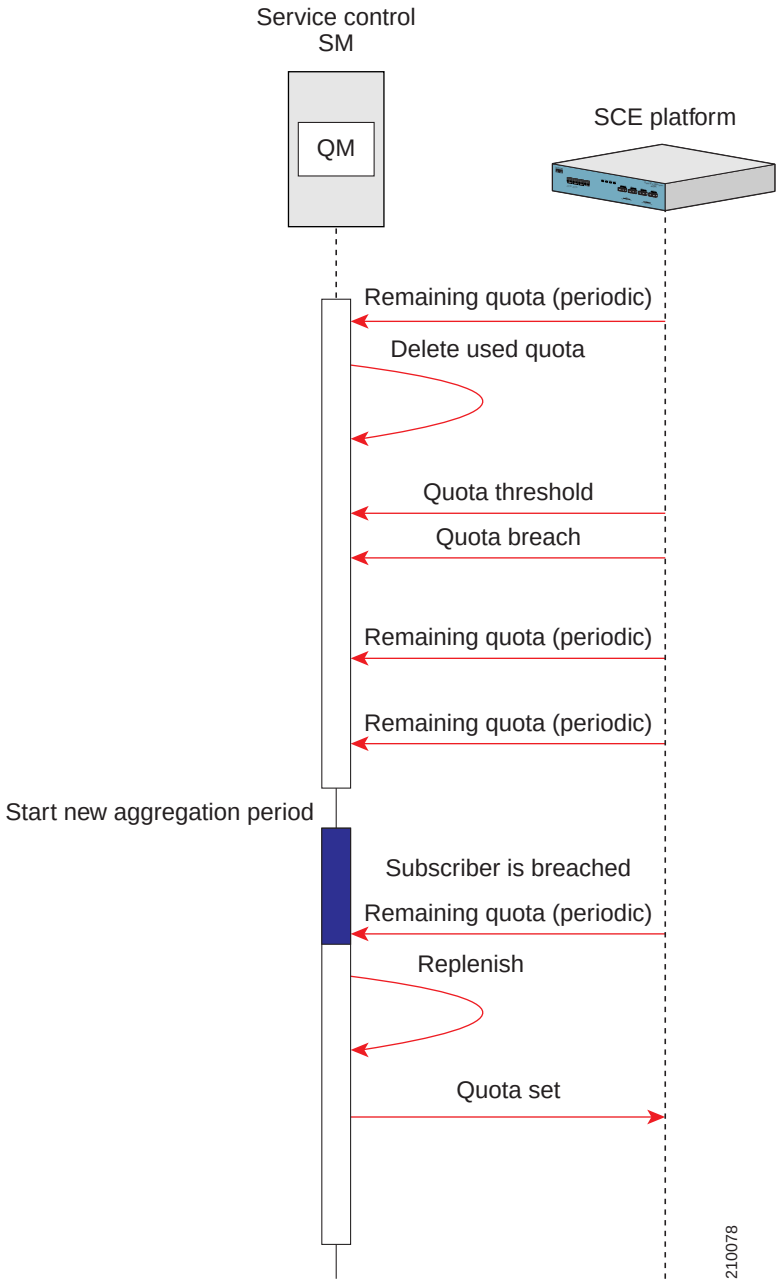
Quote Manager Images

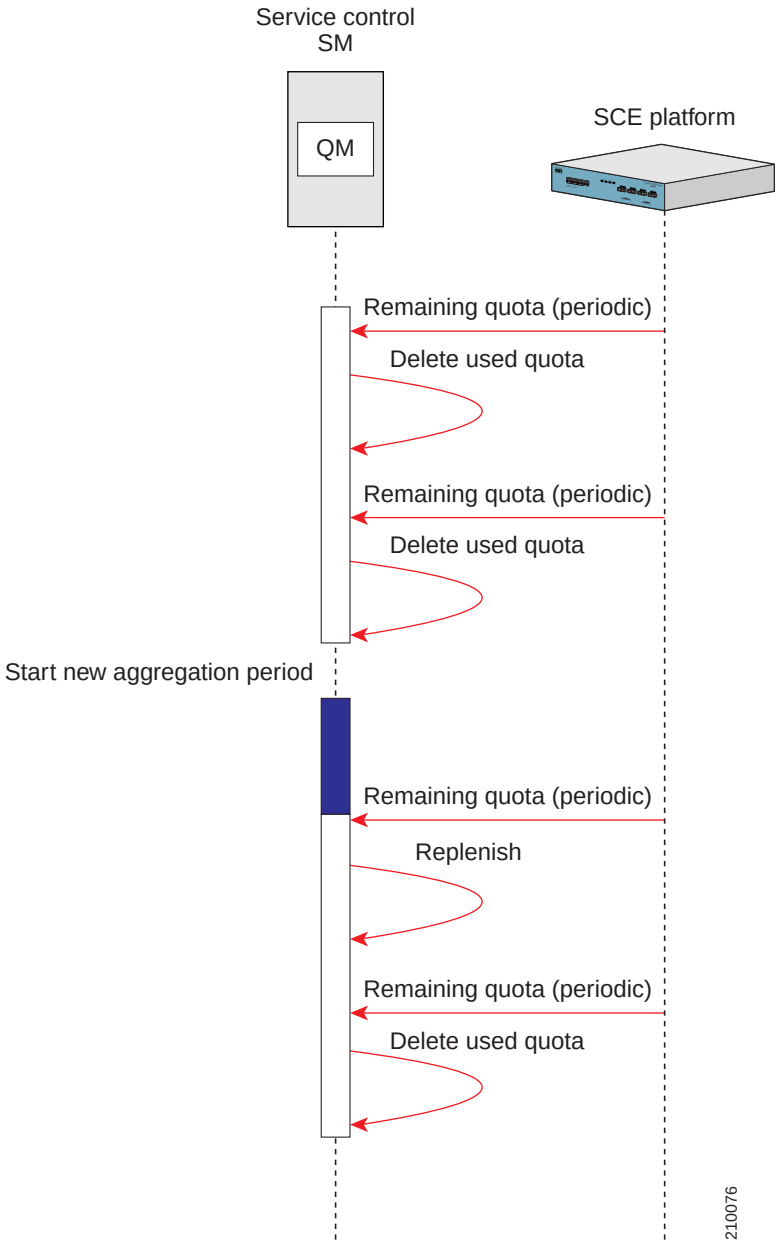


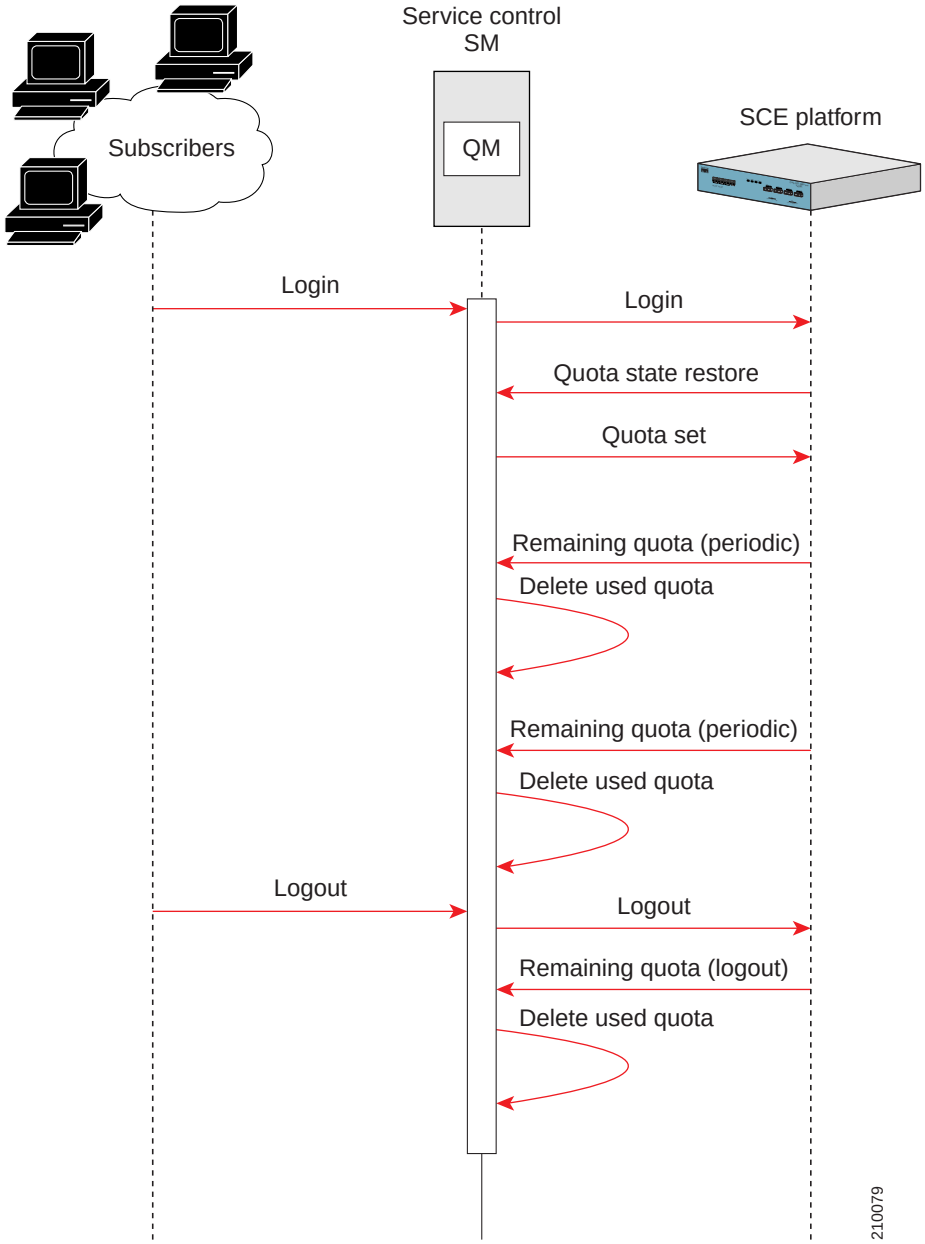

Edit Rule for Service "Default Service"
General
Control
Usage Limits
Breach Handling
Set the Quota Buckets that the Service's traffic will consume.
Select Quota Bucket for upstream traffic
Bucket 1
Select Quota Bucket for downstream traffic
Bucket 1
Select Quota Bucket for sessions
None (Unlimited)
OK
Cancel
210270

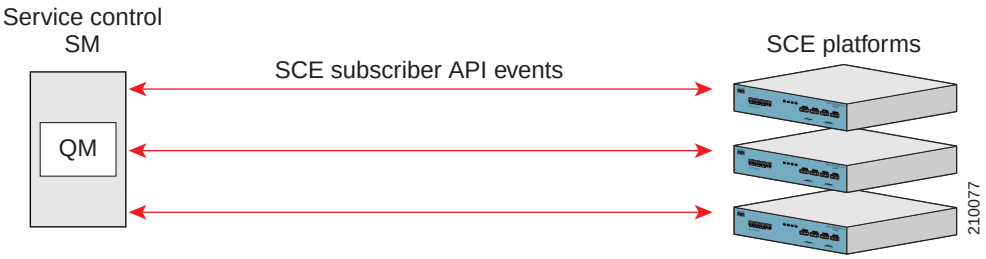

Edit Rule for Service "Default Service"
General
Control
Usage Limits
Breach Handling
In case a subscriber's usage exceeded the volume or number of sessions limits:
No changes to active control
Block the flow
Redirect to
Default set
Control the flow's characteristics:
Select an upstream Bandwidth Controller
Default Upstream BWC
Select a downstream Bandwidth Controller
Default Downstream BWC
Limit the flow's upstream bandwidth to
Kbps
Limit the flow's downstream bandwidth to
Kbps
Limit concurrent flows of this Service to
Activate a Subscriber Notification:
Default Notification
OK
Cancel
210269

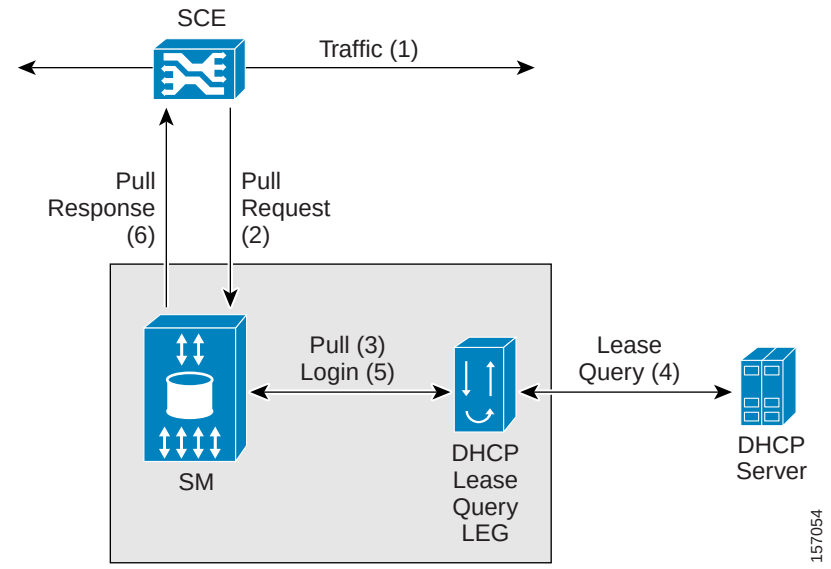

Package Settings for "Default Package"
General
Quota Management
Subscriber BW Controllers
Advanced
Select quota management mode:
External - replenished on external request
Periodical - replenished automatically at the end of the aggregation period
Aggregation Period
Hourly - ends on the hour
Daily - ends at midnight
Quota Buckets
Buckets define limits on the volume and session consumption of a subscriber.
Bucket ID
Name
Type
Quota Limit
1 Bucket 1 Volume (L3 KBytes) Set Externally
2 Bucket 2 Volume (L3 KBytes) Set Externally
3 Bucket 3 Volume (L3 KBytes) Set Externally
4 Bucket 4 Volume (L3 KBytes) Set Externally
5 Bucket 5 Volume (L3 KBytes) Set Externally
OK
Cancel
210271

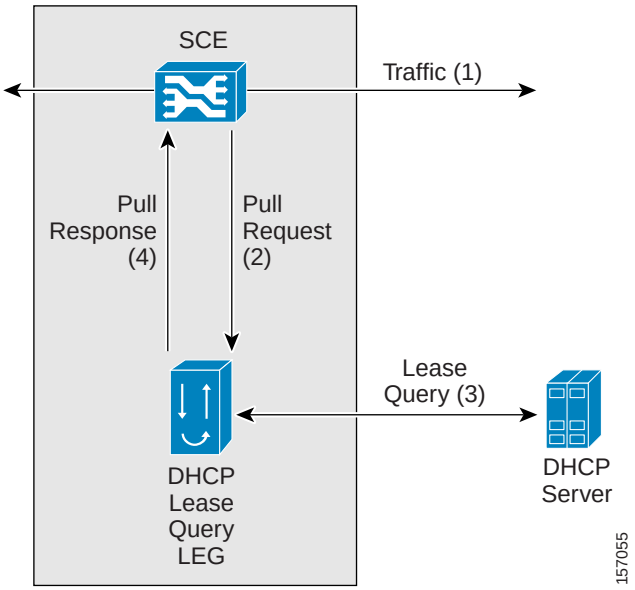

Service control
SM
QM
SCE platform
Remaining quota (periodic)
Delete used quota
Quota threshold
Quota breach
Remaining quota (periodic)
Remaining quota (periodic)
Start new aggregation period
Subscriber is breached
Remaining quota (periodic)
Replenish
Quota set
210078

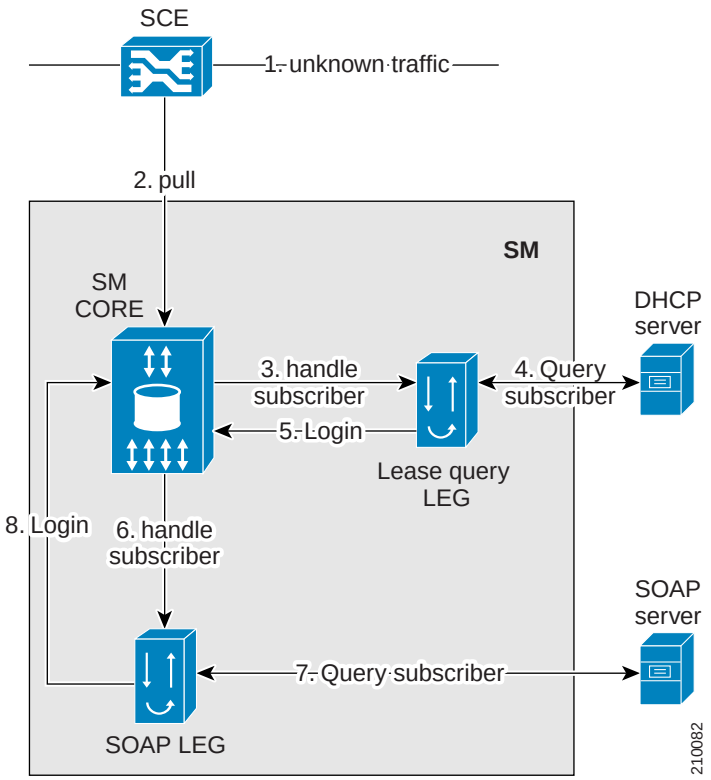

Service control
SM
QM
SCE platform
Remaining quota (periodic)
Delete used quota
Remaining quota (periodic)
Delete used quota
Start new aggregation period
Remaining quota (periodic)
Replenish
Remaining quota (periodic)
Delete used quota
210076

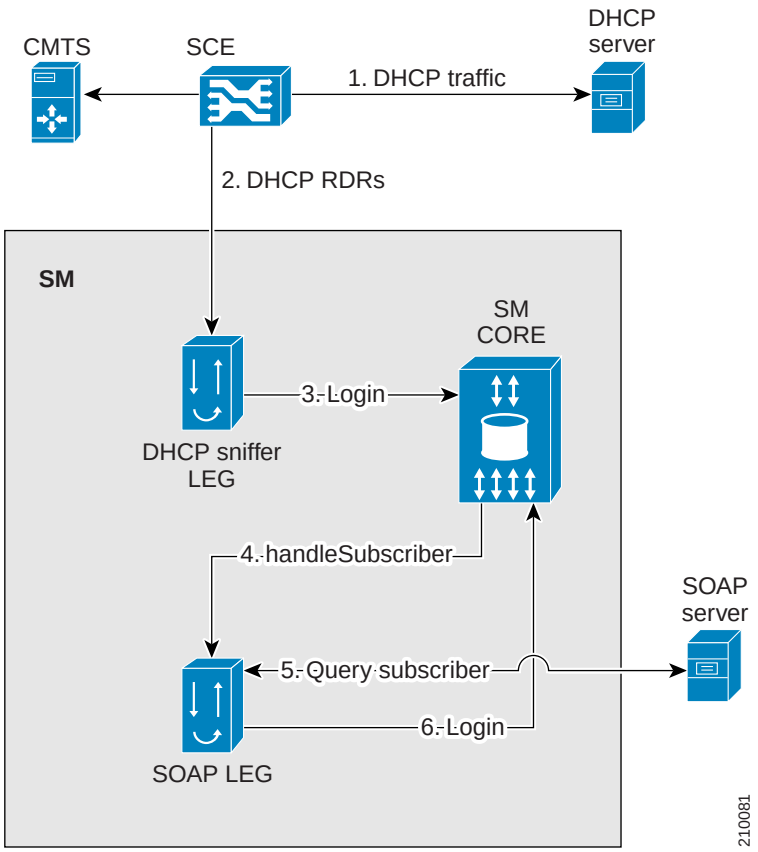

Service control
SM
Subscribers
QM
SCE platform
Login
Login
Quota state restore
Quota set
Remaining quota (periodic)
Delete used quota
Remaining quota (periodic)
Delete used quota
Logout
Logout
Remaining quota (logout)
Delete used quota
210079

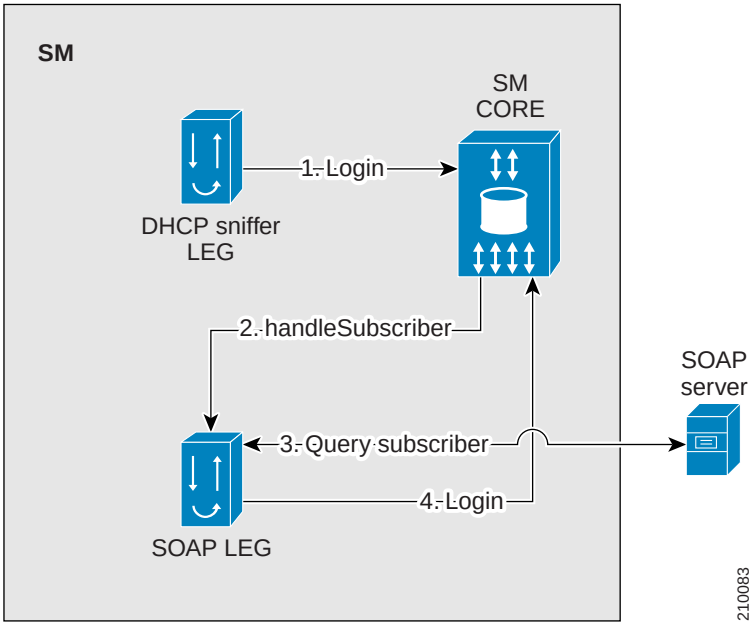

Service control
SM
QM
SCE subscriber API events
SCE platforms
210077

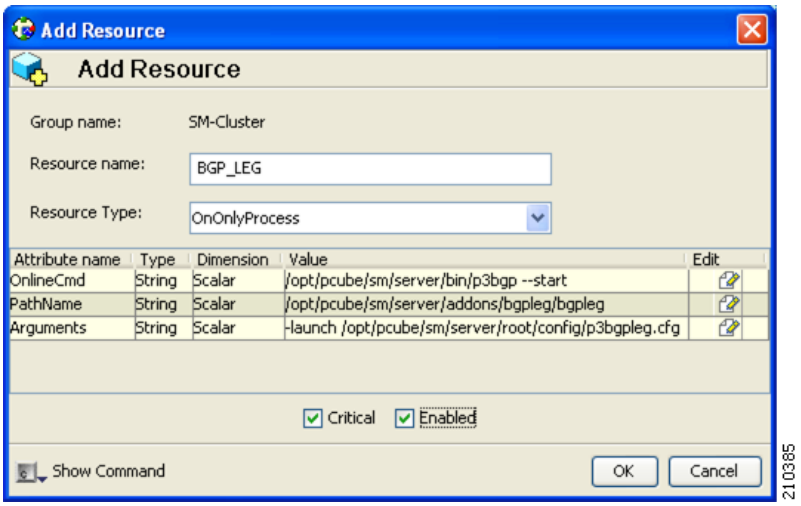

SCE
Traffic (1)
Pull
Response
(6)
Pull
Request
(2)
Pull (3)
Login (5)
Lease
Query (4)
SM
DHCP
Lease
Query
LEG
DHCP
Server
157054

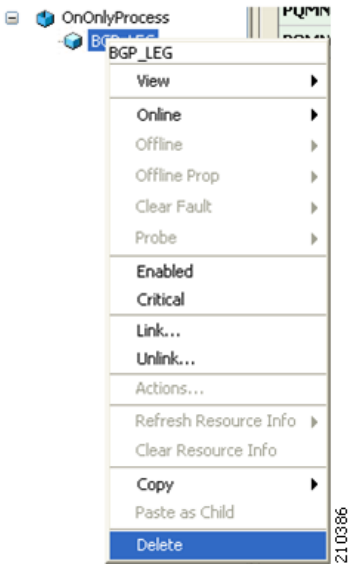

SCE
Traffic (1)
Pull
Response
(4)
Pull
Request
(2)
Lease
Query (3)
DHCP
Lease
Query
LEG
DHCP
Server
157055

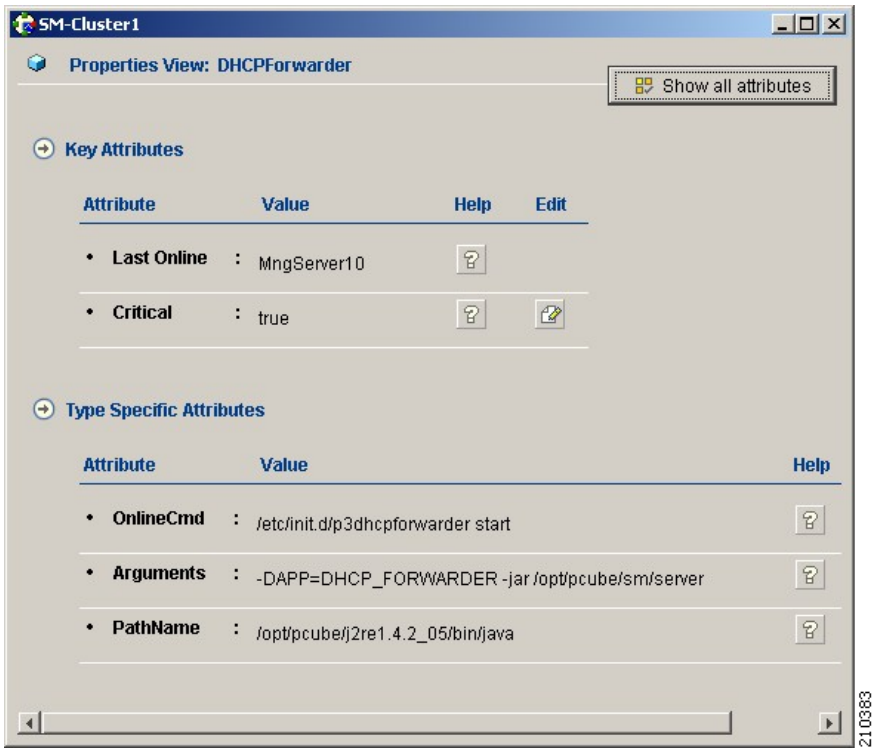

SCE
1. unknown traffic
2. pull
SM
SM CORE
DHCP server
3. handle subscriber
4. Query subscriber
5. Login
Lease query LEG
8. Login
6. handle subscriber
SOAP server
7. Query subscriber
SOAP LEG
210082

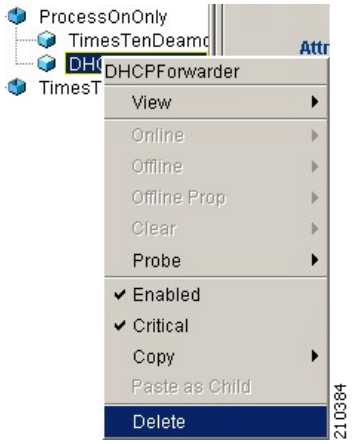

CMTS
SCE
DHCP server
1. DHCP traffic
2. DHCP RDRs
SM
SM CORE
3. Login
DHCP sniffer LEG
4. handleSubscriber
SOAP server
5. Query subscriber
6. Login
SOAP LEG
210081

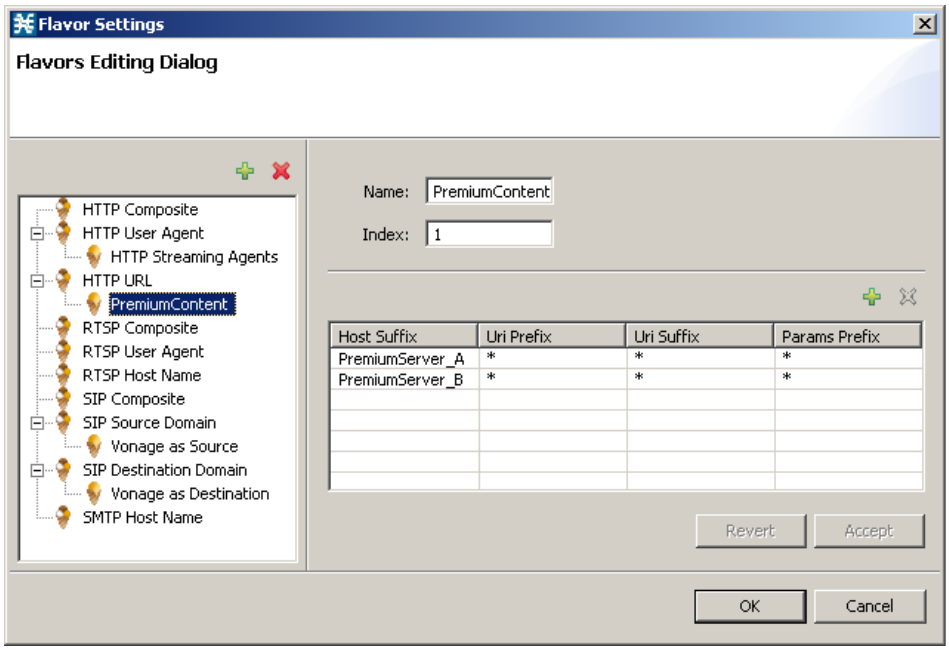

SM
SM CORE
1. Login
DHCP sniffer LEG
2. handleSubscriber
SOAP server
3. Query subscriber
4. Login
SOAP LEG
210083

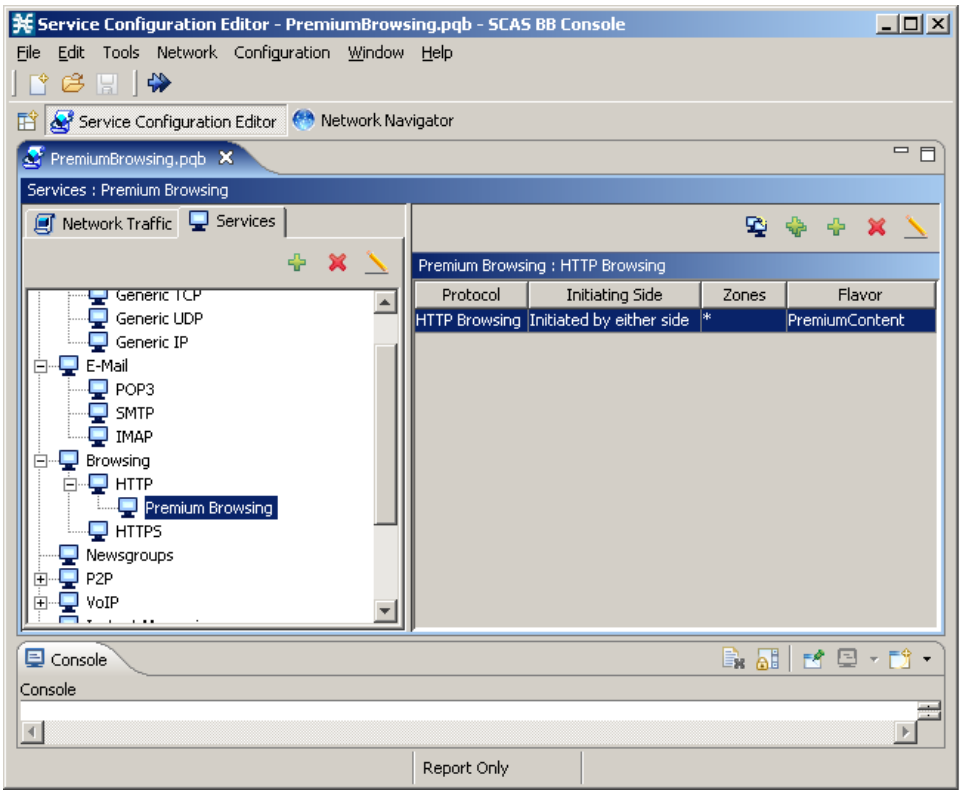

Add Resource
Add Resource
Group name:
SM-Cluster
Resource name:
BGP_LEG
Resource Type:
OnOnlyProcess
Attribute name
Type
Dimension
Value
Edit
OnlineCmd
String
Scalar
/opt/pcube/sm/server/bin/p3bgp --start
PathName
String
Scalar
/opt/pcube/sm/server/addons/bgpleg/bgpleg
Arguments
String
Scalar
-launch /opt/pcube/sm/server/root/config/p3bgpleg.cfg
Critical
Enabled
Show Command
OK
Cancel
210385

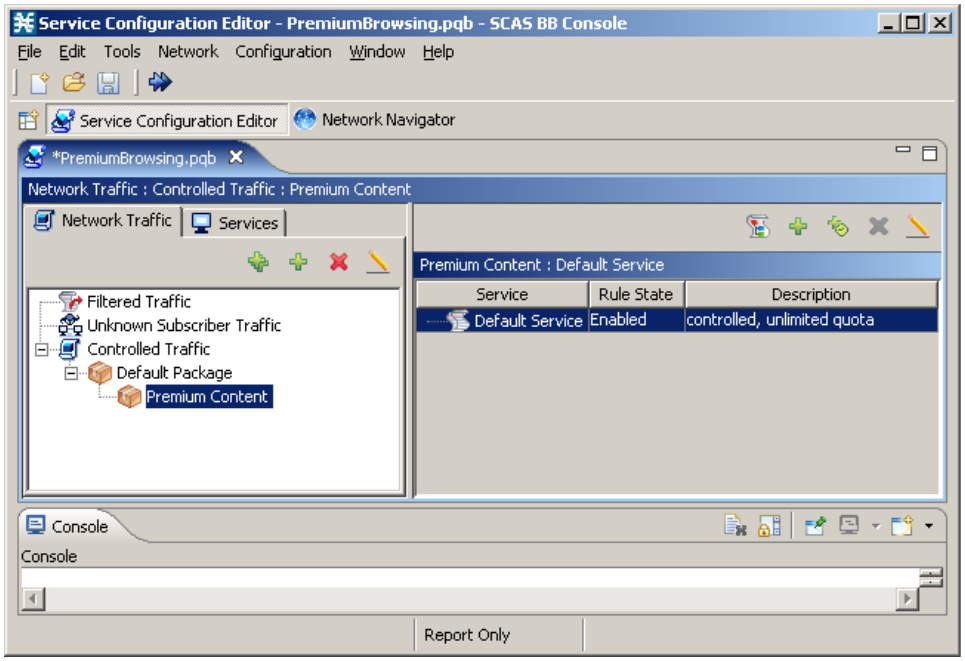

OnOnlyProcess
BGP_LEG
View
Online
Offline
Offline Prop
Clear Fault
Probe
Enabled
Critical
Link...
Unlink...
Actions...
Refresh Resource Info
Clear Resource Info
Copy
Paste as Child
Delete
210386

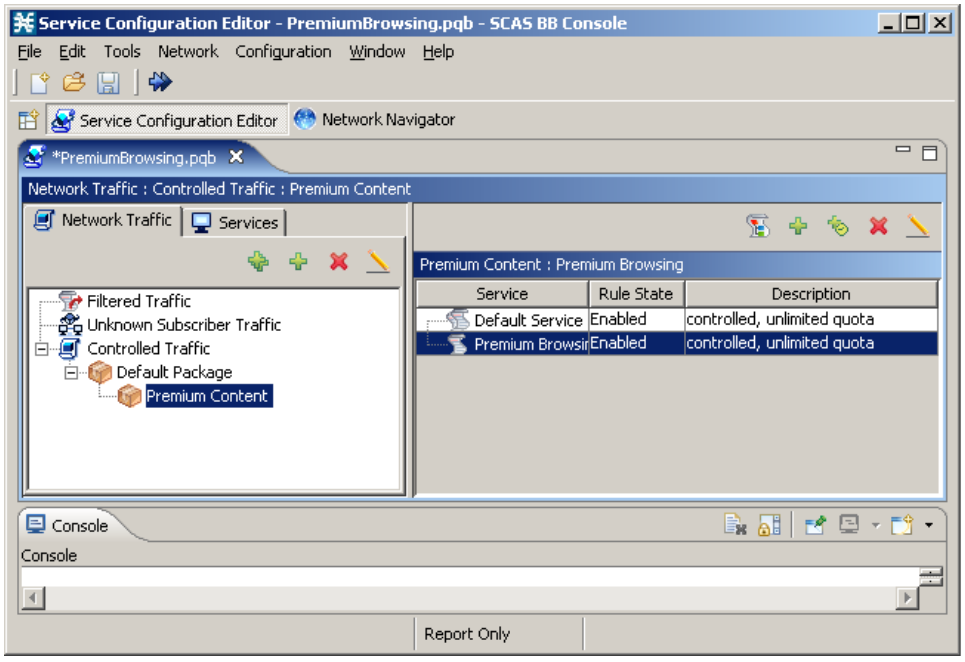

SM-Cluster1
Properties View: DHCPForwarder
Show all attributes
Key Attributes
Attribute
Value
Help
Edit
Last Online : MngServer10
Critical : true
Type Specific Attributes
Attribute
Value
Help
OnlineCmd : /etc/init.d/p3dhcpforwarder start
Arguments : -DAPP=DHCP_FORWARDER -jar /opt/pcube/sm/server
PathName : /opt/pcube/j2re1.4.2_05/bin/java
210383

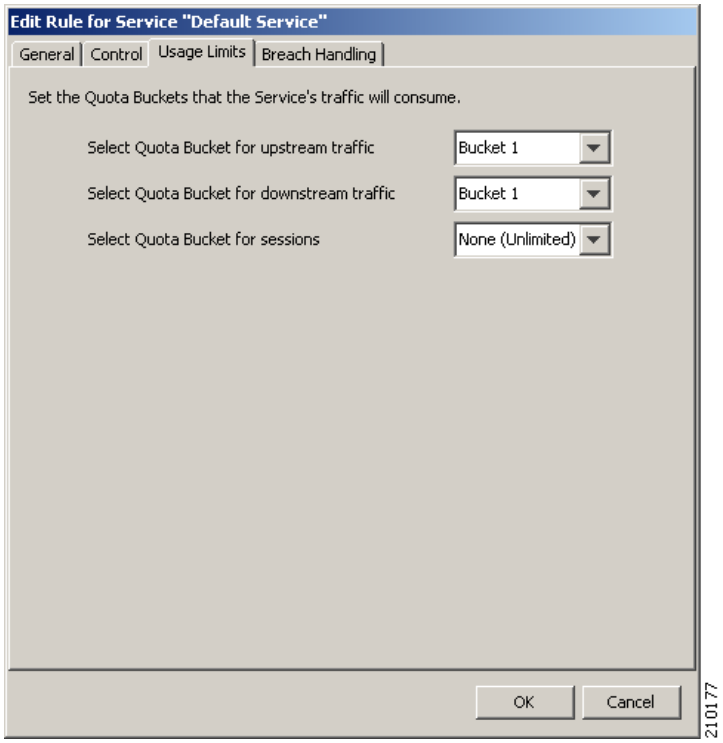

ProcessOnOnly
TimesTenDeamc
DHC
TimesT
Attr
DHCPForwarder
View
Online
Offline
Offline Prop
Clear
Probe
Enabled
Critical
Copy
Paste as Child
Delete
210384

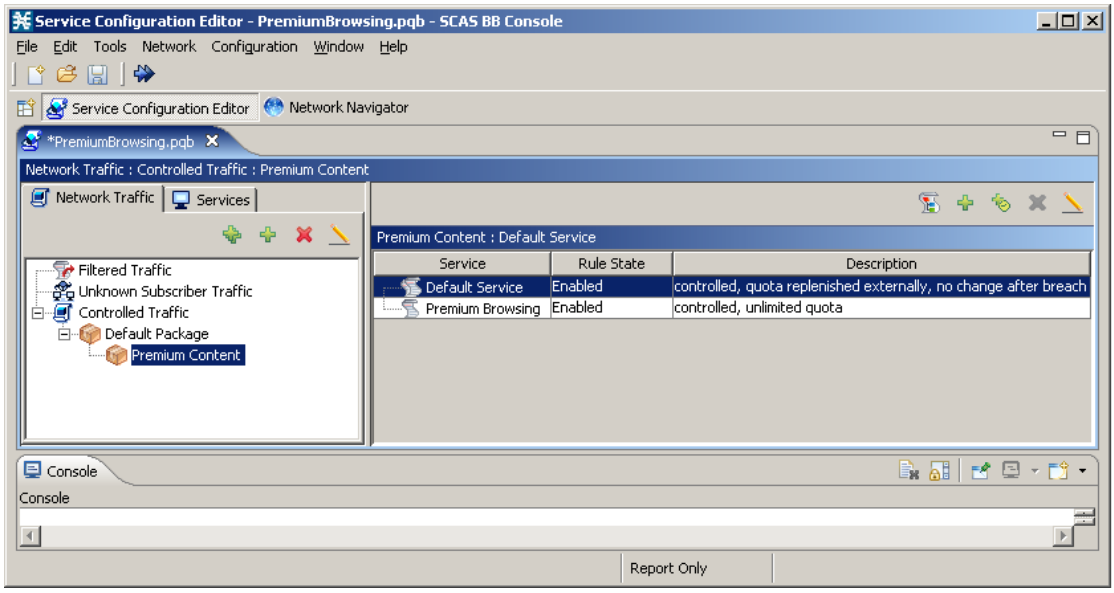

Flavor Settings
Flavors Editing Dialog
HTTP Composite
HTTP User Agent
HTTP Streaming Agents
HTTP URL
PremiumContent
RTSP Composite
RTSP User Agent
RTSP Host Name
SIP Composite
SIP Source Domain
Vonage as Source
SIP Destination Domain
Vonage as Destination
SMTP Host Name
Name: PremiumContent
Index: 1
Host Suffix
Uri Prefix
Uri Suffix
Params Prefix
PremiumServer_A
PremiumServer_B
Revert
Accept
OK
Cancel
210178

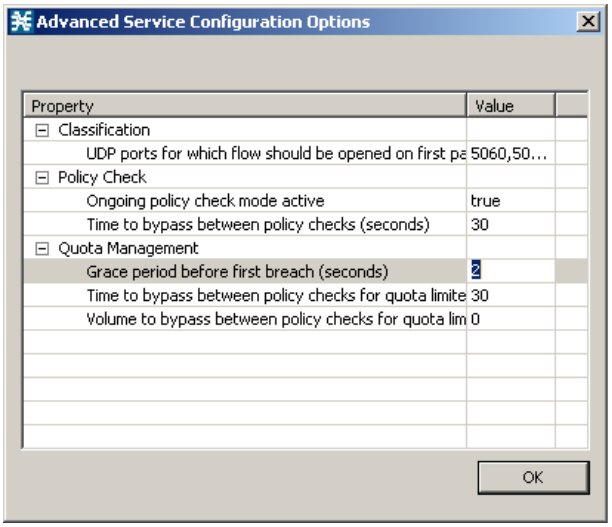

Service Configuration Editor - PremiumBrowsing.pqb - SCAS BB Console
File Edit Tools Network Configuration Window Help
Service Configuration Editor
Network Navigator
PremiumBrowsing.pqb
Services : Premium Browsing
Network Traffic
Services
Generic UDP
Generic IP
E-Mail
POP3
SMTP
IMAP
Browsing
HTTP
Premium Browsing
HTTPS
Newsgroups
P2P
VoIP
Premium Browsing : HTTP Browsing
Protocol
Initiating Side
Zones
Flavor
HTTP Browsing
Initiated by either side
*
PremiumContent
Console
Report Only
210181

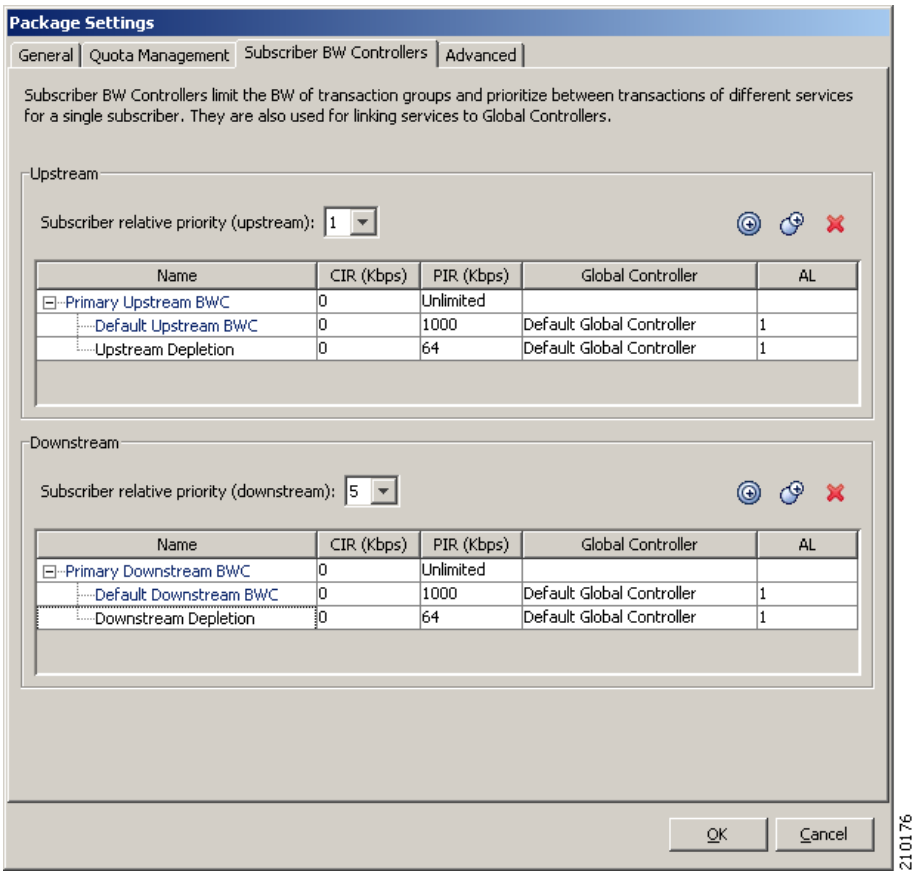

Service Configuration Editor - PremiumBrowsing.pqb - SCAS BB Console
File Edit Tools Network Configuration Window Help
Service Configuration Editor
Network Navigator
*PremiumBrowsing.pqb
Network Traffic : Controlled Traffic : Premium Content
Network Traffic
Services
Filtered Traffic
Unknown Subscriber Traffic
Controlled Traffic
Default Package
Premium Content
Premium Content : Default Service
Service
Rule State
Description
Default Service
Enabled
controlled, unlimited quota
Console
Console
Report Only
210179

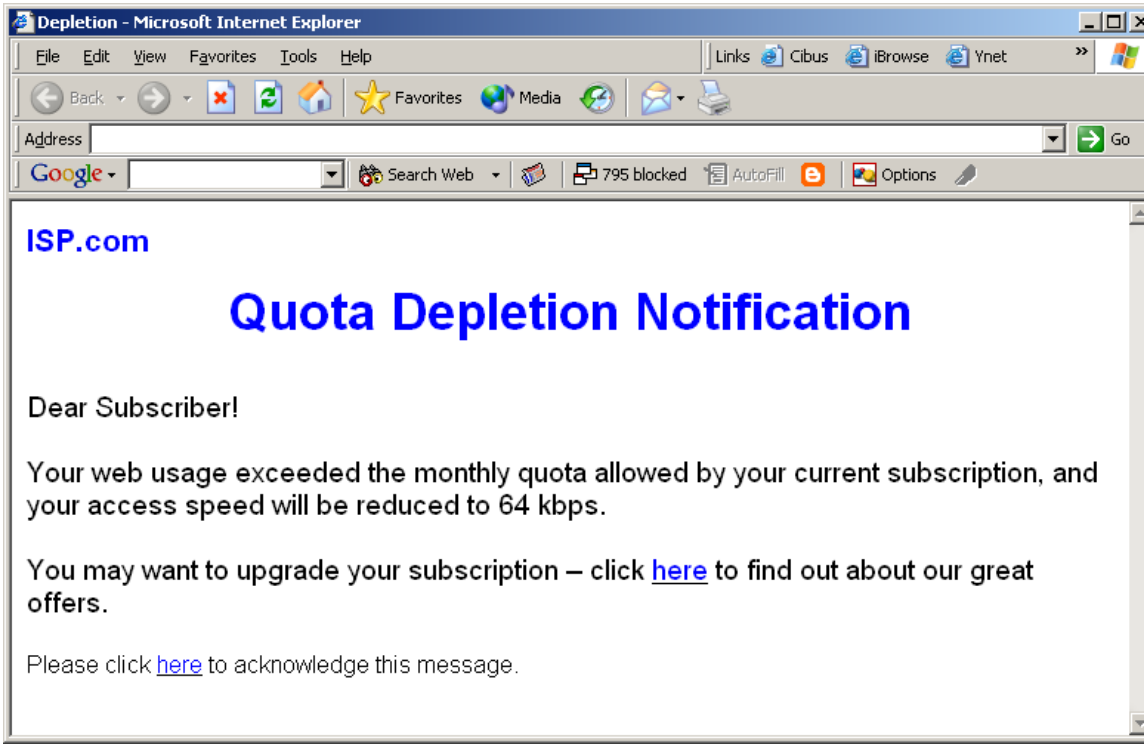

Service Configuration Editor - PremiumBrowsing.pqb - SCAS BB Console
File Edit Tools Network Configuration Window Help
Service Configuration Editor
Network Navigator
*PremiumBrowsing.pqb
Network Traffic : Controlled Traffic : Premium Content
Network Traffic
Services
Filtered Traffic
Unknown Subscriber Traffic
Controlled Traffic
Default Package
Premium Content
Premium Content : Premium Browsing
Service
Rule State
Description
Default Service
Enabled
controlled, unlimited quota
Premium Browsir
Enabled
controlled, unlimited quota
Console
Console
Report Only
210180

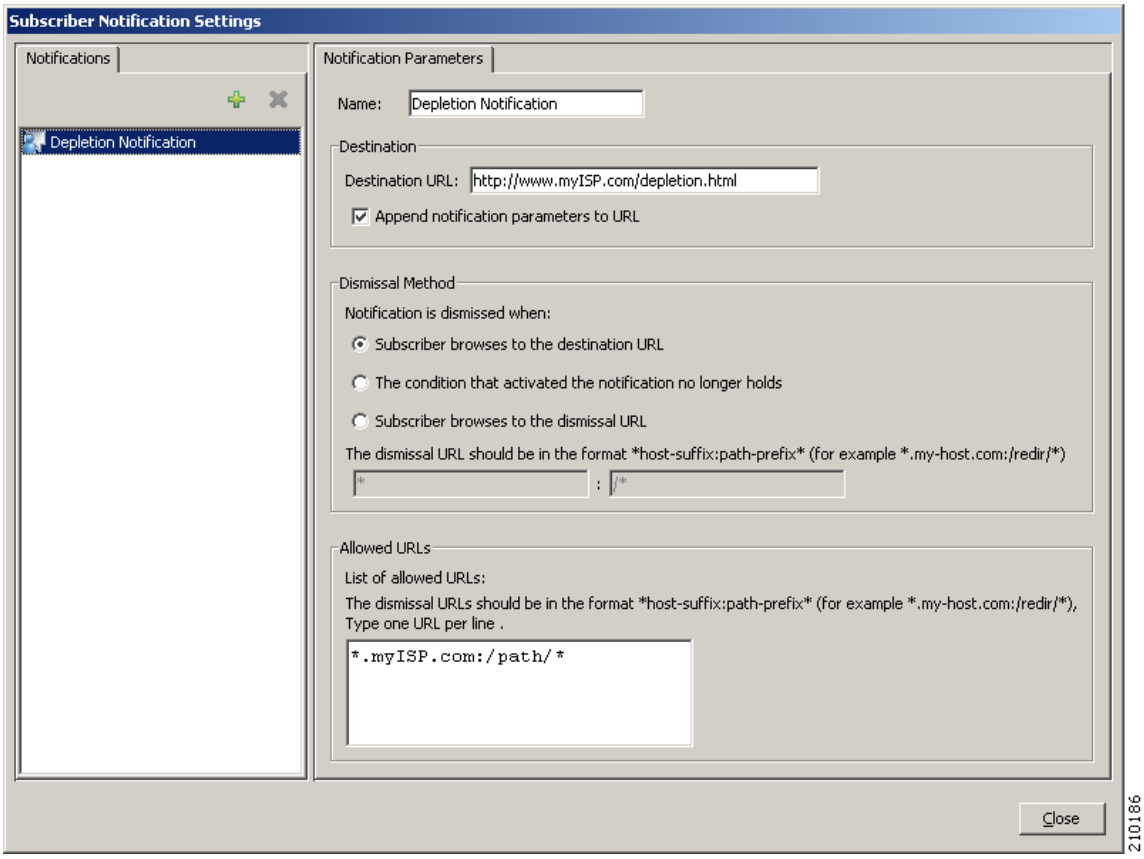

Edit Rule for Service "Default Service"
General
Control
Usage Limits
Breach Handling
Set the Quota Buckets that the Service's traffic will consume.
Select Quota Bucket for upstream traffic
Bucket 1
Select Quota Bucket for downstream traffic
Bucket 1
Select Quota Bucket for sessions
None (Unlimited)
OK
Cancel
210177

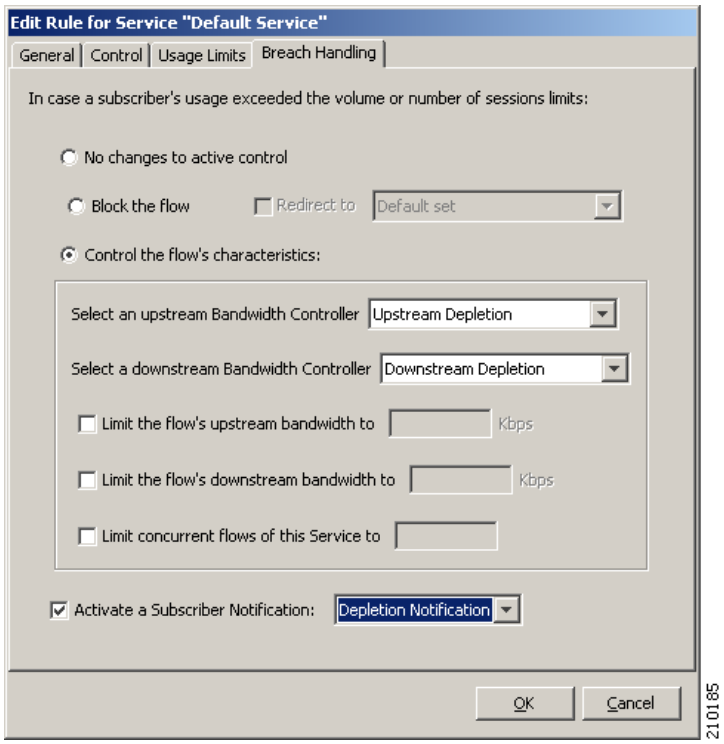

Service Configuration Editor - PremiumBrowsing.pqb - SCAS BB Console
File
Edit
Tools
Network
Configuration
Window
Help
Service Configuration Editor
Network Navigator
*PremiumBrowsing.pqb
Network Traffic : Controlled Traffic : Premium Content
Network Traffic
Services
Filtered Traffic
Unknown Subscriber Traffic
Controlled Traffic
Default Package
Premium Content
Premium Content : Default Service
Service
Rule State
Description
Default Service
Enabled
controlled, quota replenished externally, no change after breach
Premium Browsing
Enabled
controlled, unlimited quota
Console
Console
Report Only
210182

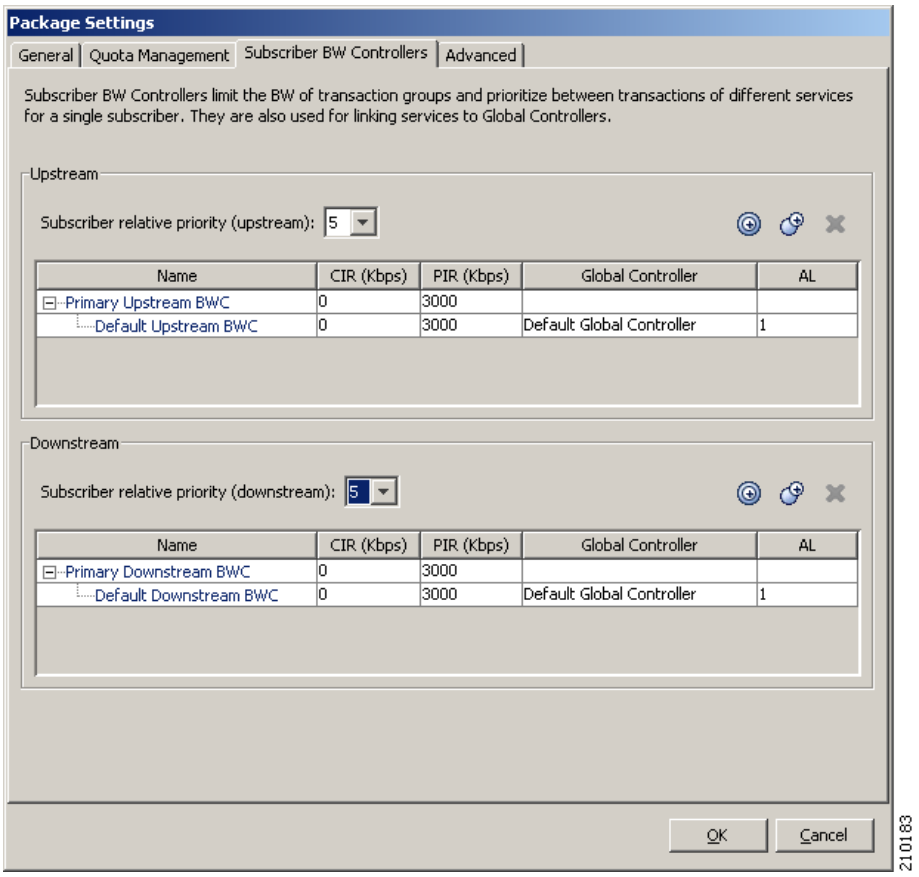

Advanced Service Configuration Options
Property
Value
Classification
UDP ports for which flow should be opened on first pa
5060,50...
Policy Check
Ongoing policy check mode active
true
Time to bypass between policy checks (seconds)
30
Quota Management
Grace period before first breach (seconds)
2
Time to bypass between policy checks for quota limite
30
Volume to bypass between policy checks for quota lim
0
OK
210175

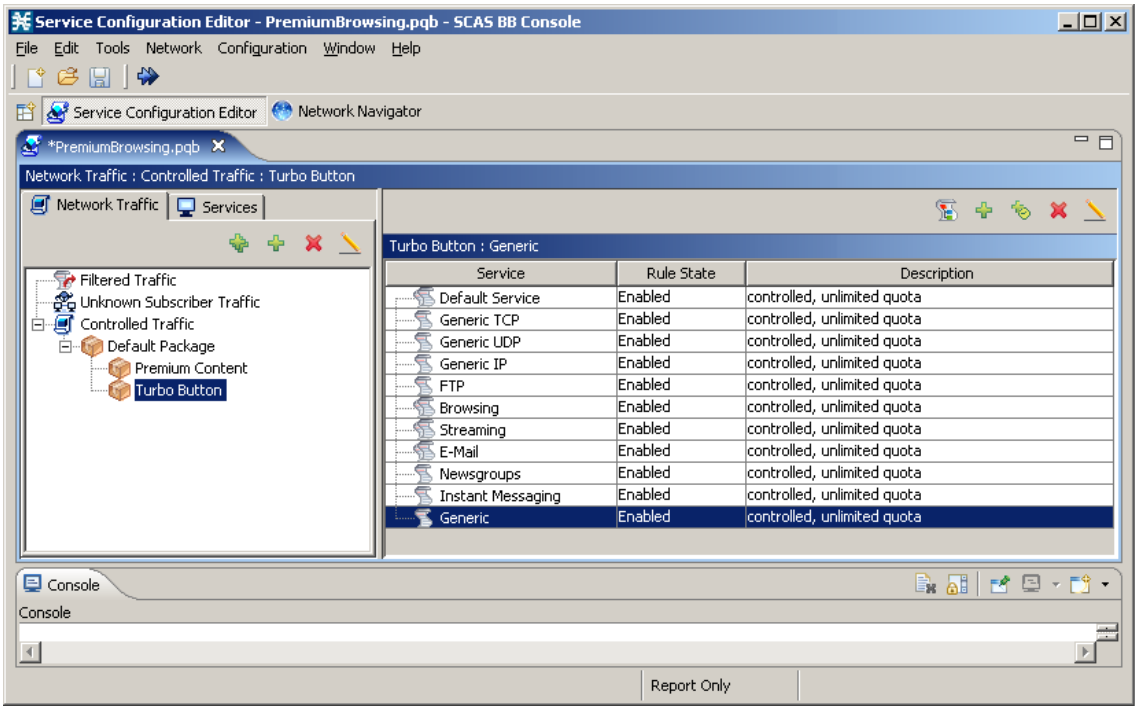

Package Settings
General
Quota Management
Subscriber BW Controllers
Advanced
Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.
Upstream
Subscriber relative priority (upstream):
1
Name
CIR (Kbps)
PIR (Kbps)
Global Controller
AL
Primary Upstream BWC
0
Unlimited
Default Upstream BWC
0
1000
Default Global Controller
1
Upstream Depletion
0
64
Default Global Controller
1
Downstream
Subscriber relative priority (downstream):
5
Name
CIR (Kbps)
PIR (Kbps)
Global Controller
AL
Primary Downstream BWC
0
Unlimited
Default Downstream BWC
0
1000
Default Global Controller
1
Downstream Depletion
0
64
Default Global Controller
1
OK
Cancel
210176

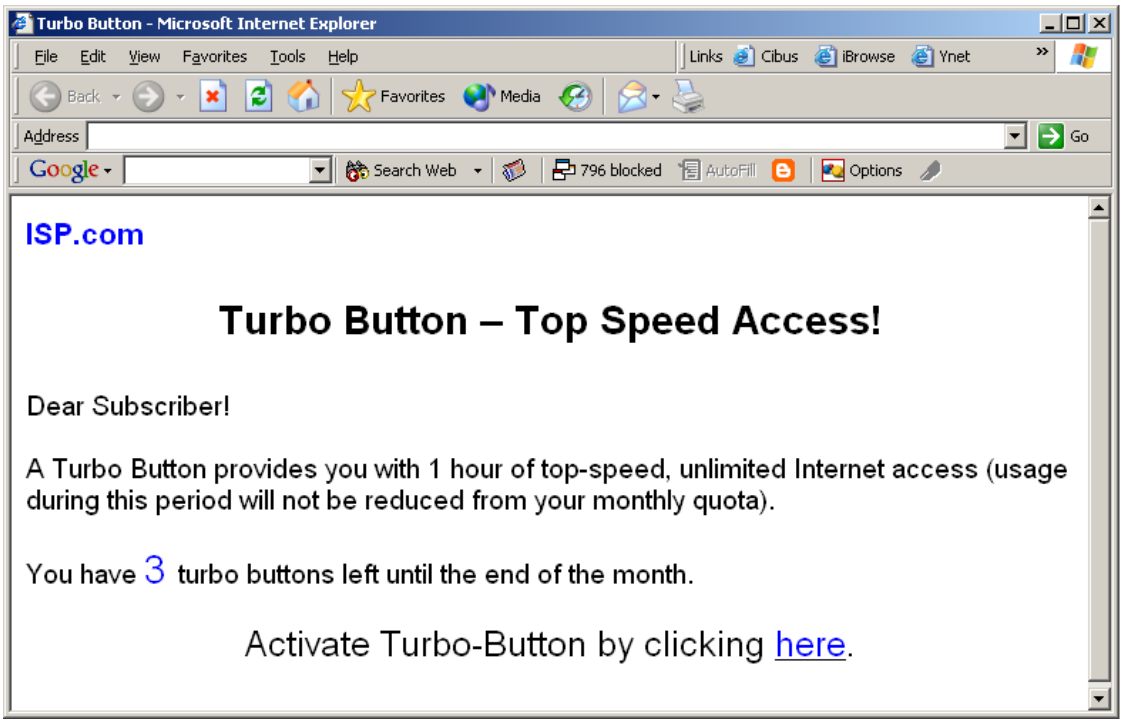

Depletion - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links Cibus iBrowse Ynet
Back Favorites Media
Address
Go
Google Search Web 795 blocked AutoFill Options
ISP.com
Quota Depletion Notification
Dear Subscriber!
Your web usage exceeded the monthly quota allowed by your current subscription, and your access speed will be reduced to 64 kbps.
You may want to upgrade your subscription – click here to find out about our great offers.
Please click here to acknowledge this message.

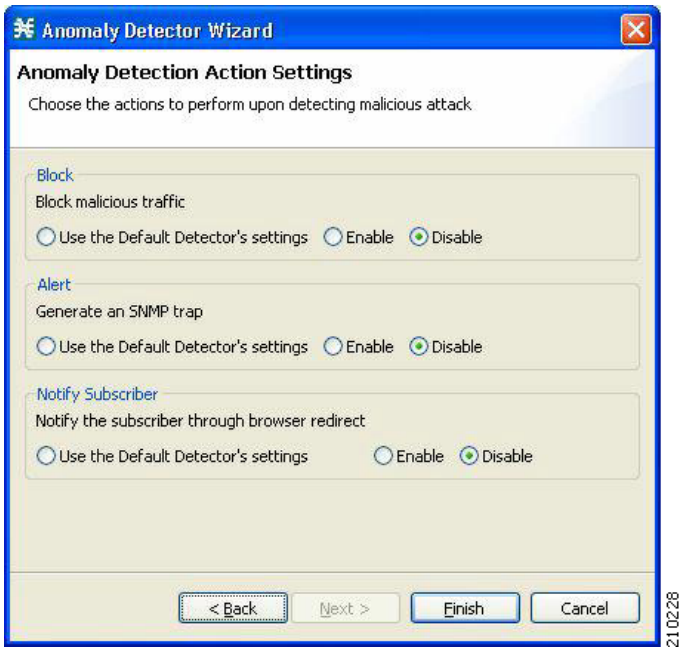

Subscriber Notification Settings
Notifications
Depletion Notification
Notification Parameters
Name:
Depletion Notification
Destination
Destination URL:
http://www.myISP.com/depletion.html
Append notification parameters to URL
Dismissal Method
Notification is dismissed when:
Subscriber browses to the destination URL
The condition that activated the notification no longer holds
Subscriber browses to the dismissal URL
The dismissal URL should be in the format *host-suffix:path-prefix* (for example *.my-host.com:/redir/*)
Allowed URLs
List of allowed URLs:
The dismissal URLs should be in the format *host-suffix:path-prefix* (for example *.my-host.com:/redir/*), Type one URL per line .
.myISP.com:/path/
Close
210186

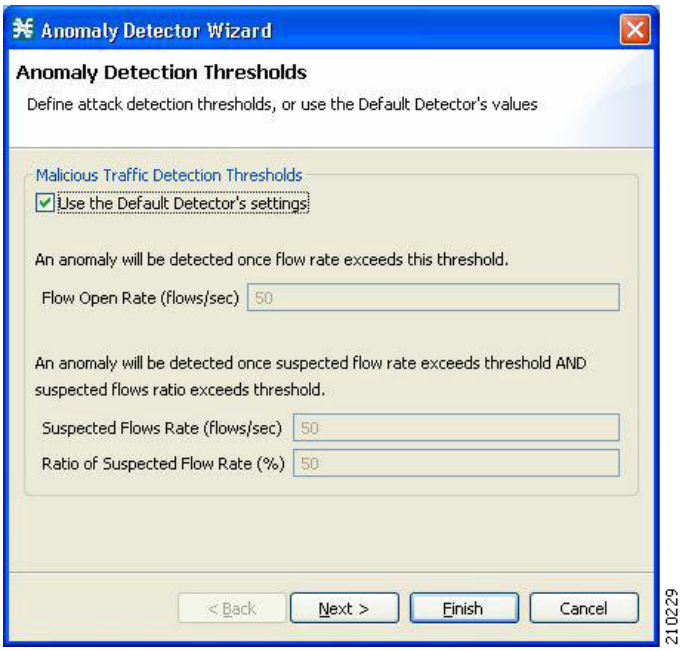

Edit Rule for Service "Default Service"
General
Control
Usage Limits
Breach Handling
In case a subscriber's usage exceeded the volume or number of sessions limits:
No changes to active control
Block the flow
Redirect to
Default set
Control the flow's characteristics:
Select an upstream Bandwidth Controller
Upstream Depletion
Select a downstream Bandwidth Controller
Downstream Depletion
Limit the flow's upstream bandwidth to
Kbps
Limit the flow's downstream bandwidth to
Kbps
Limit concurrent flows of this Service to
Activate a Subscriber Notification:
Depletion Notification
OK
Cancel
210185

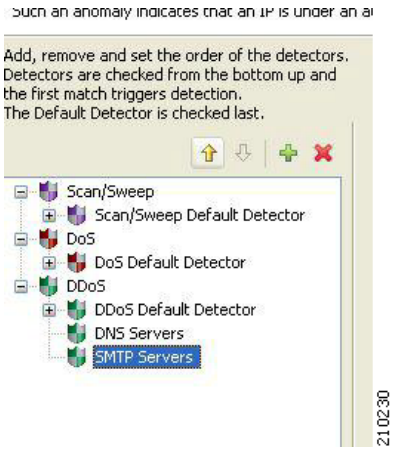

Package Settings
General
Quota Management
Subscriber BW Controllers
Advanced
Subscriber BW Controllers limit the BW of transaction groups and prioritize between transactions of different services for a single subscriber. They are also used for linking services to Global Controllers.
Upstream
Subscriber relative priority (upstream): 5
Name
CIR (Kbps)
PIR (Kbps)
Global Controller
AL
Primary Upstream BWC
0
3000
Default Upstream BWC
0
3000
Default Global Controller
1
Downstream
Subscriber relative priority (downstream): 5
Name
CIR (Kbps)
PIR (Kbps)
Global Controller
AL
Primary Downstream BWC
0
3000
Default Downstream BWC
0
3000
Default Global Controller
1
OK
Cancel
210183

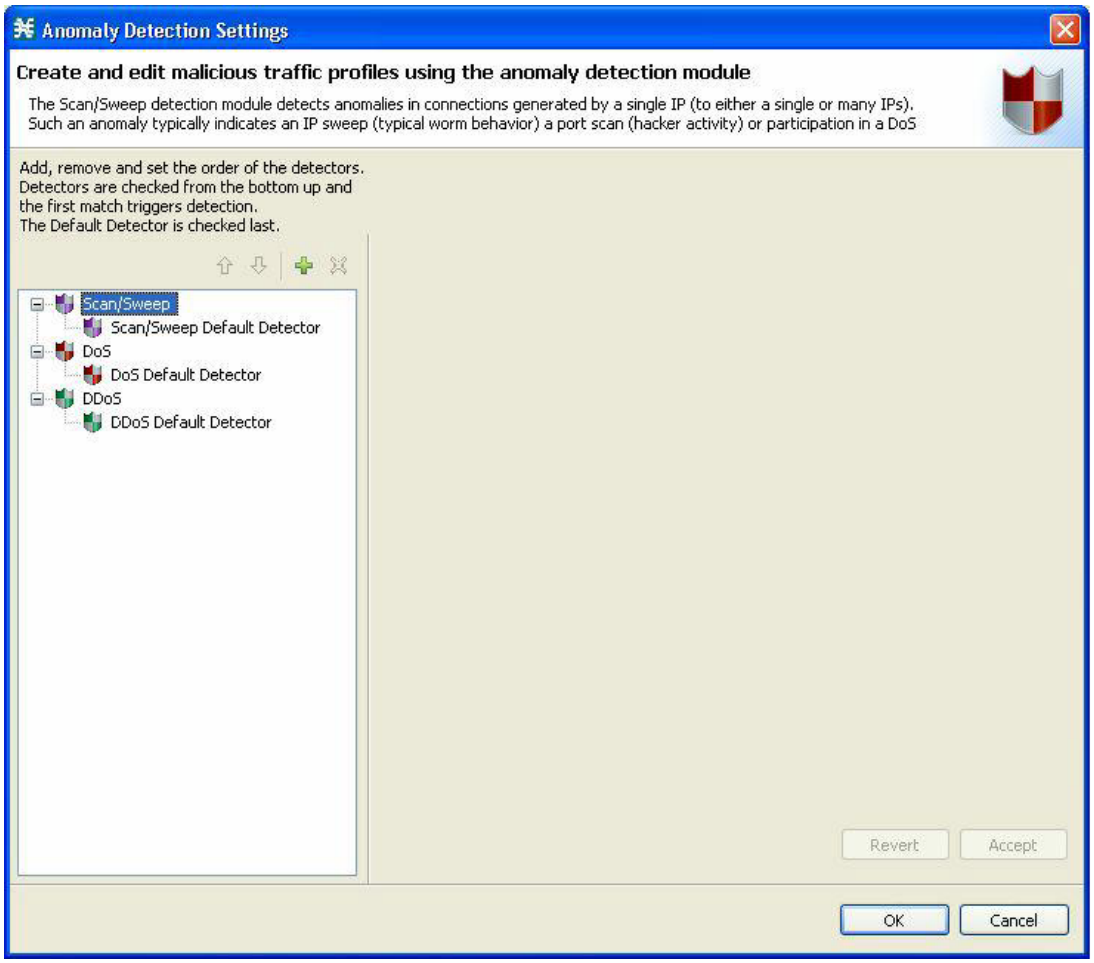

Service Configuration Editor - PremiumBrowsing.pqb - SCAS BB Console
File Edit Tools Network Configuration Window Help
Service Configuration Editor
Network Navigator
*PremiumBrowsing.pqb
Network Traffic : Controlled Traffic : Turbo Button
Network Traffic
Services
Filtered Traffic
Unknown Subscriber Traffic
Controlled Traffic
Default Package
Premium Content
Turbo Button
Turbo Button : Generic
Service
Rule State
Description
Default Service Enabled controlled, unlimited quota
Generic TCP Enabled controlled, unlimited quota
Generic UDP Enabled controlled, unlimited quota
Generic IP Enabled controlled, unlimited quota
FTP Enabled controlled, unlimited quota
Browsing Enabled controlled, unlimited quota
Streaming Enabled controlled, unlimited quota
E-Mail Enabled controlled, unlimited quota
Newsgroups Enabled controlled, unlimited quota
Instant Messaging Enabled controlled, unlimited quota
Generic Enabled controlled, unlimited quota
Console
Console
Report Only

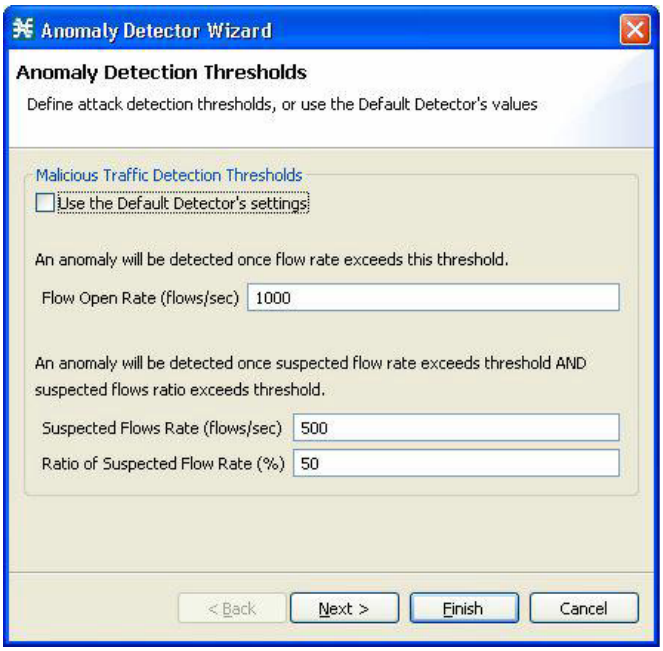

Turbo Button - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Links Cibus iBrowse Ynet
Back
Favorites
Media
Address
Go
Google
Search Web
796 blocked
AutoFill
Options
ISP.com
Turbo Button – Top Speed Access!
Dear Subscriber!
A Turbo Button provides you with 1 hour of top-speed, unlimited Internet access (usage during this period will not be reduced from your monthly quota).
You have 3 turbo buttons left until the end of the month.
Activate Turbo-Button by clicking here.
210187

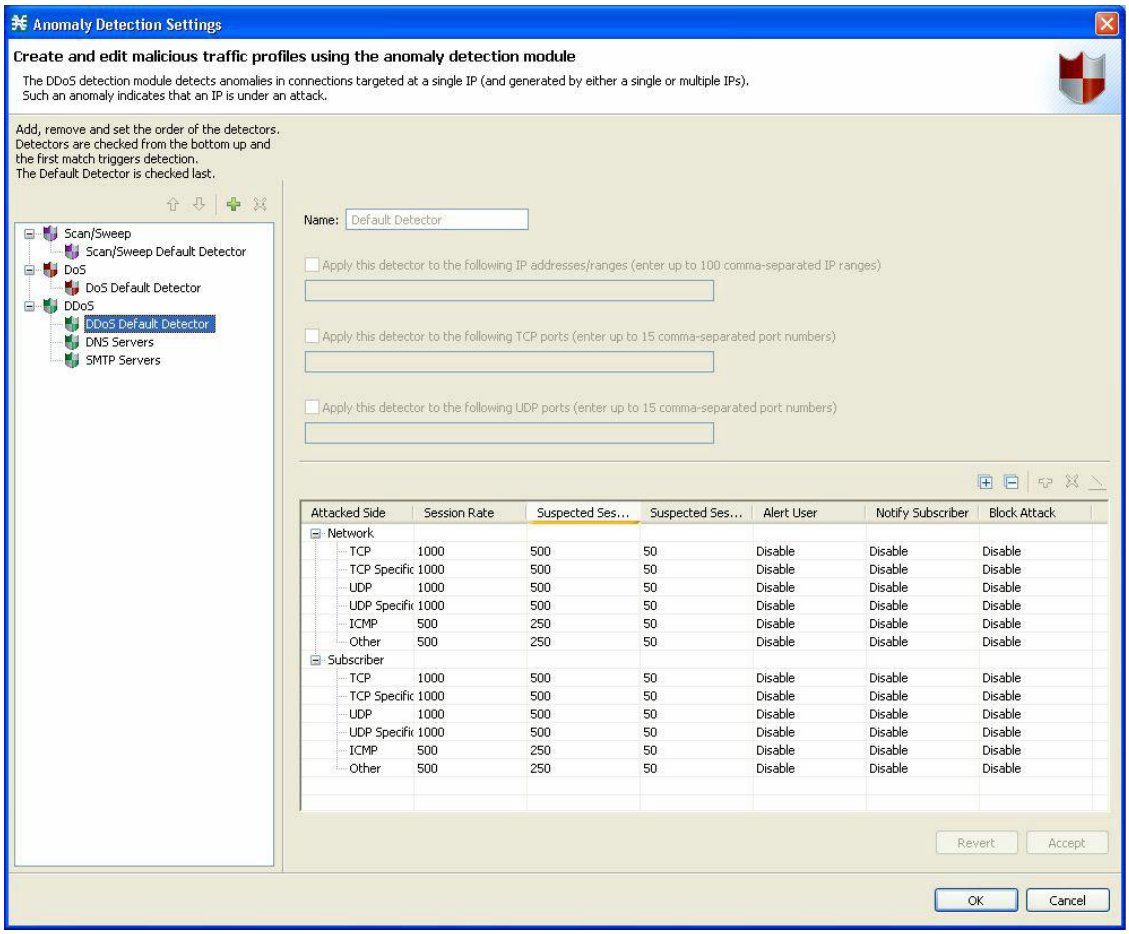

Anomaly Detector Wizard
Anomaly Detection Action Settings
Choose the actions to perform upon detecting malicious attack
Block
Block malicious traffic
Use the Default Detector's settings
Enable
Disable
Alert
Generate an SNMP trap
Use the Default Detector's settings
Enable
Disable
Notify Subscriber
Notify the subscriber through browser redirect
Use the Default Detector's settings
Enable
Disable
< Back
Next >
Finish
Cancel
210228

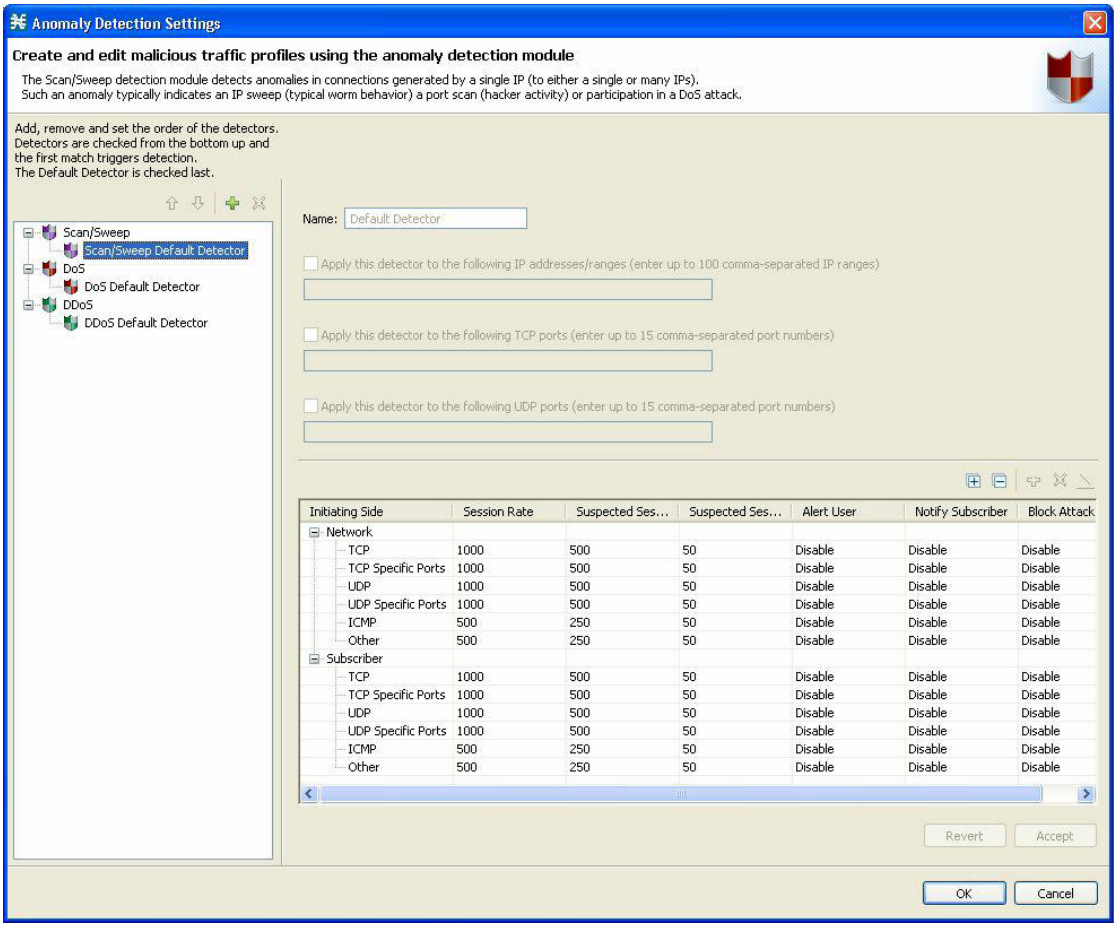

Anomaly Detector Wizard
Anomaly Detection Thresholds
Define attack detection thresholds, or use the Default Detector's values
Malicious Traffic Detection Thresholds
Use the Default Detector's settings
An anomaly will be detected once flow rate exceeds this threshold.
Flow Open Rate (flows/sec)
50
An anomaly will be detected once suspected flow rate exceeds threshold AND suspected flows ratio exceeds threshold.
Suspected Flows Rate (flows/sec)
50
Ratio of Suspected Flow Rate (%)
50
< Back
Next >
Finish
Cancel
210229

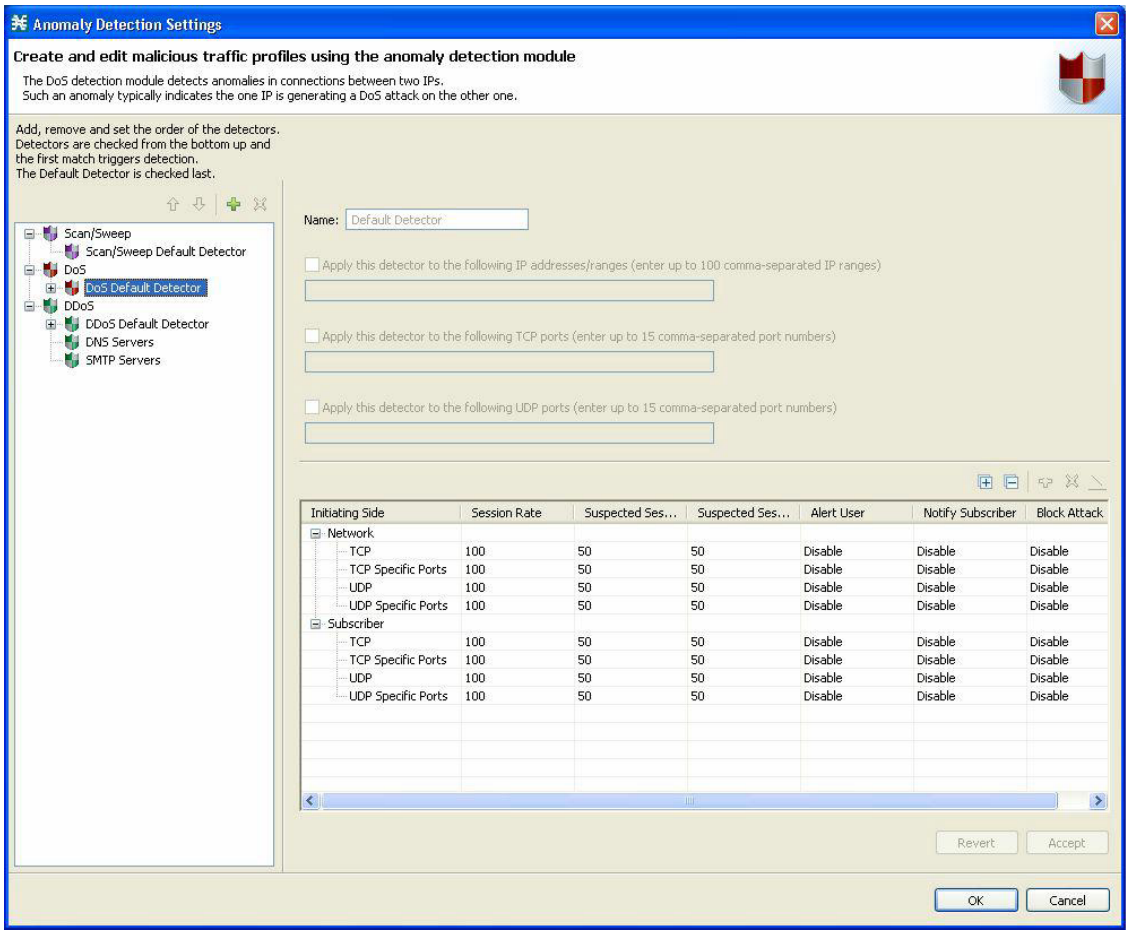

Such an anomaly indicates that an IP is under an a
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
DNS Servers
SMTP Servers
210230

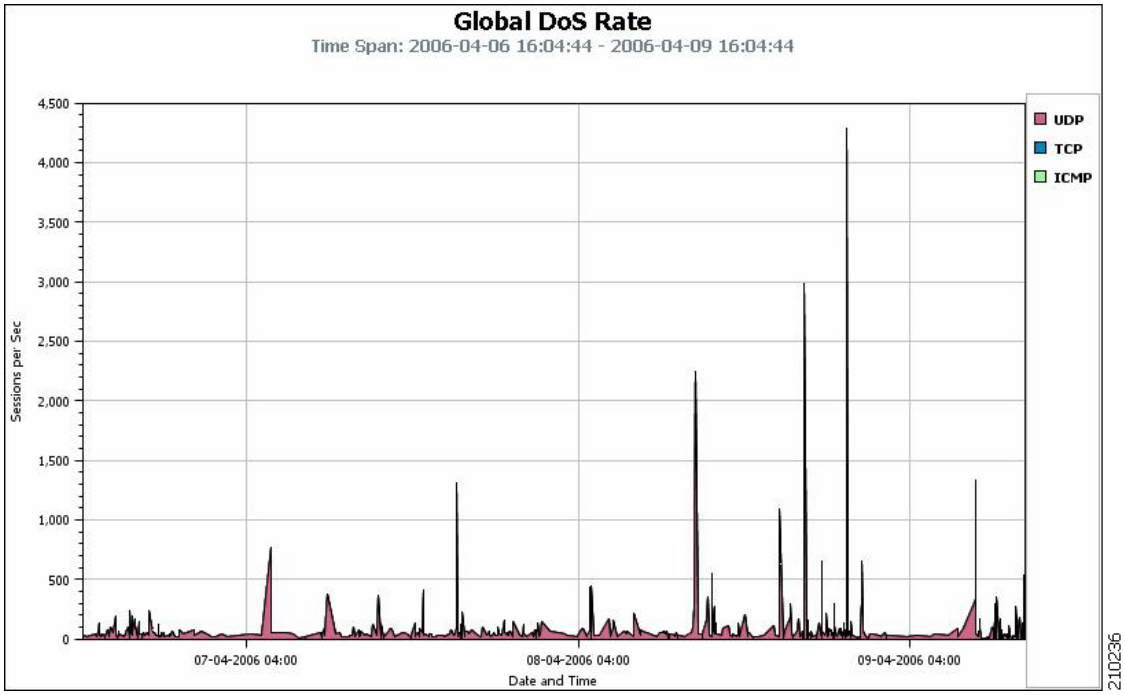

Anomaly Detection Settings
Create and edit malicious traffic profiles using the anomaly detection module
The Scan/Sweep detection module detects anomalies in connections generated by a single IP (to either a single or many IPs).
Such an anomaly typically indicates an IP sweep (typical worm behavior) a port scan (hacker activity) or participation in a DoS
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
Revert
Accept
OK
Cancel
210231

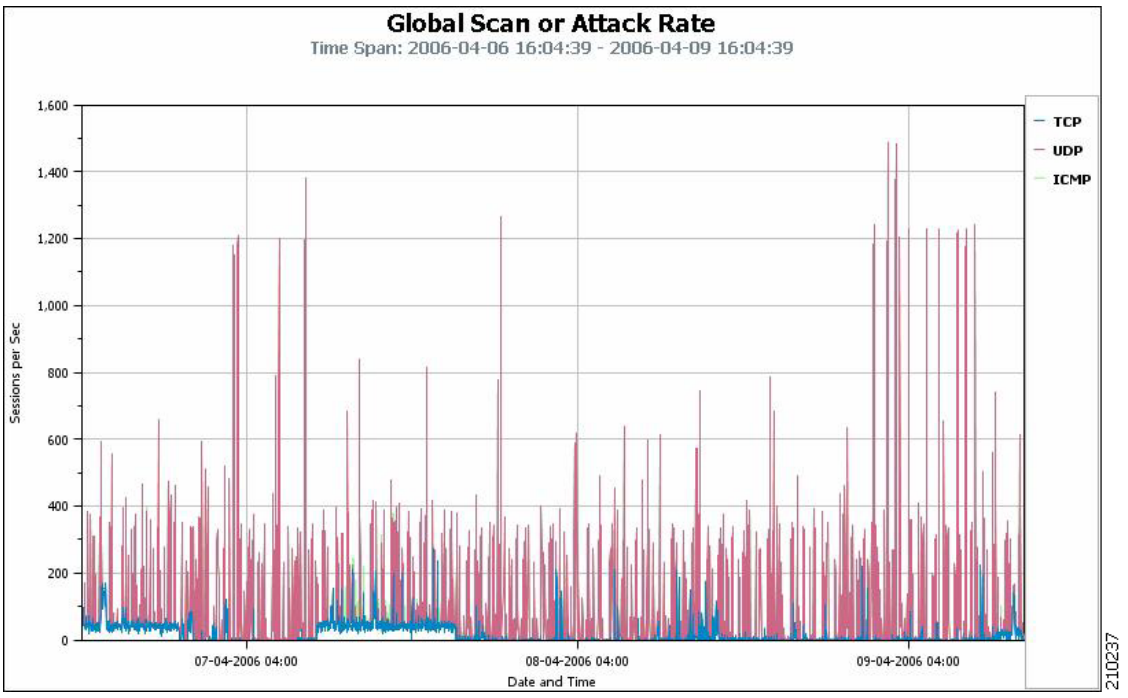

Anomaly Detector Wizard
Anomaly Detection Thresholds
Define attack detection thresholds, or use the Default Detector's values
Malicious Traffic Detection Thresholds
Use the Default Detector's settings
An anomaly will be detected once flow rate exceeds this threshold.
Flow Open Rate (flows/sec) 1000
An anomaly will be detected once suspected flow rate exceeds threshold AND suspected flows ratio exceeds threshold.
Suspected Flows Rate (flows/sec) 500
Ratio of Suspected Flow Rate (%) 50
< Back
Next >
Finish
Cancel
210232

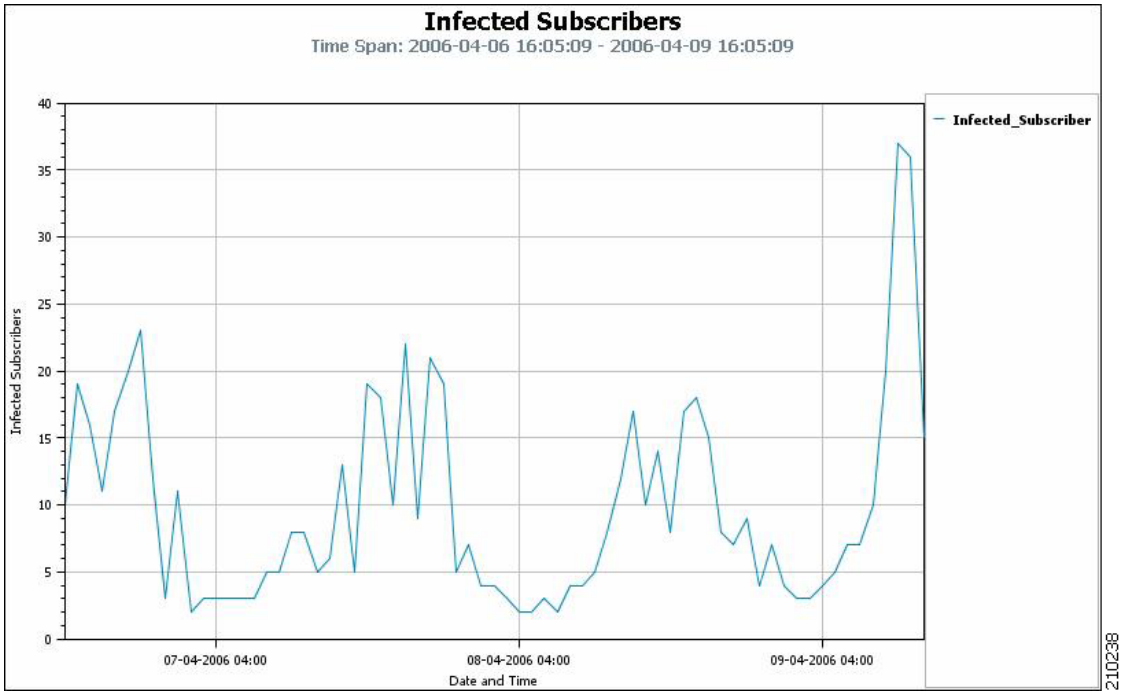

Anomaly Detection Settings
Create and edit malicious traffic profiles using the anomaly detection module
The DDoS detection module detects anomalies in connections targeted at a single IP (and generated by either a single or multiple IPs).
Such an anomaly indicates that an IP is under an attack.
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
DNS Servers
SMTP Servers
Name: Default Detector
Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)
Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)
Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)
Attacked Side | Session Rate | Suspected Ses... | Suspected Ses... | Alert User | Notify Subscriber | Block Attack
Network
TCP 1000 500 50 Disable Disable Disable
TCP Specific 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Subscriber
TCP 1000 500 50 Disable Disable Disable
TCP Specific 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Revert
Accept
OK
Cancel
210233

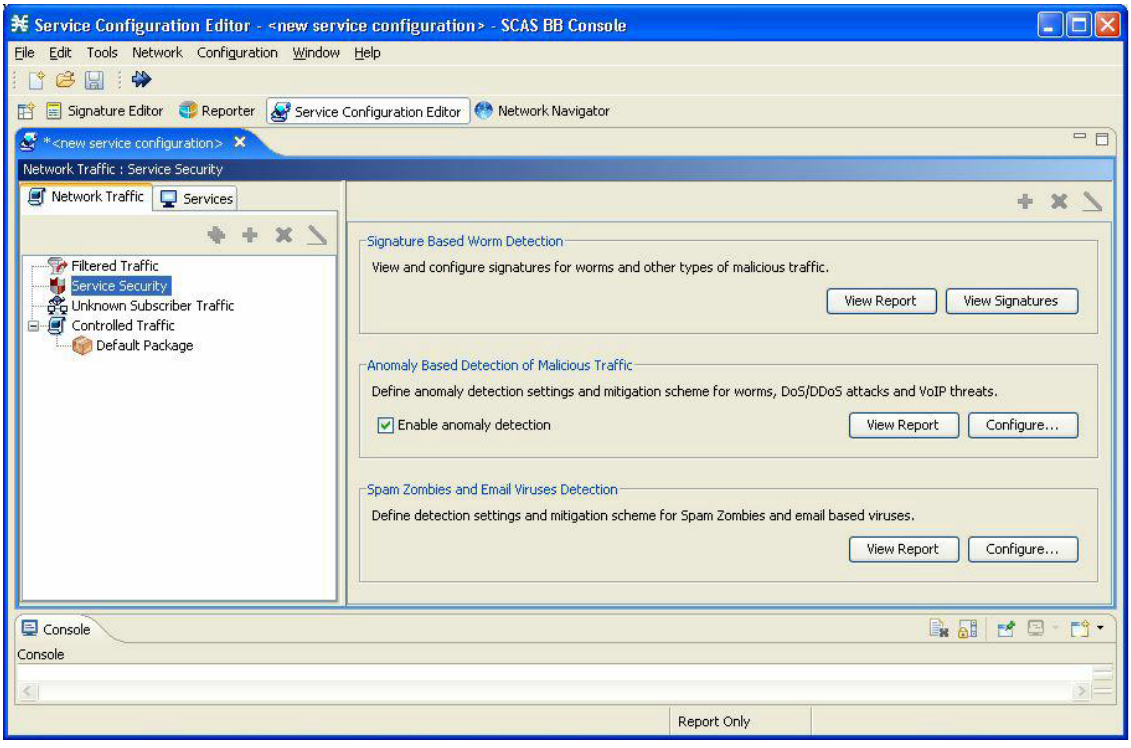

Anomaly Detection Settings
Create and edit malicious traffic profiles using the anomaly detection module
The Scan/Sweep detection module detects anomalies in connections generated by a single IP (to either a single or many IPs).
Such an anomaly typically indicates an IP sweep (typical worm behavior) a port scan (hacker activity) or participation in a DoS attack.
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
Name: Default Detector
Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)
Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)
Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)
Initiating Side | Session Rate | Suspected Ses... | Suspected Ses... | Alert User | Notify Subscriber | Block Attack
Network
TCP 1000 500 50 Disable Disable Disable
TCP Specific Ports 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific Ports 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Subscriber
TCP 1000 500 50 Disable Disable Disable
TCP Specific Ports 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific Ports 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Revert
Accept
OK
Cancel
210234

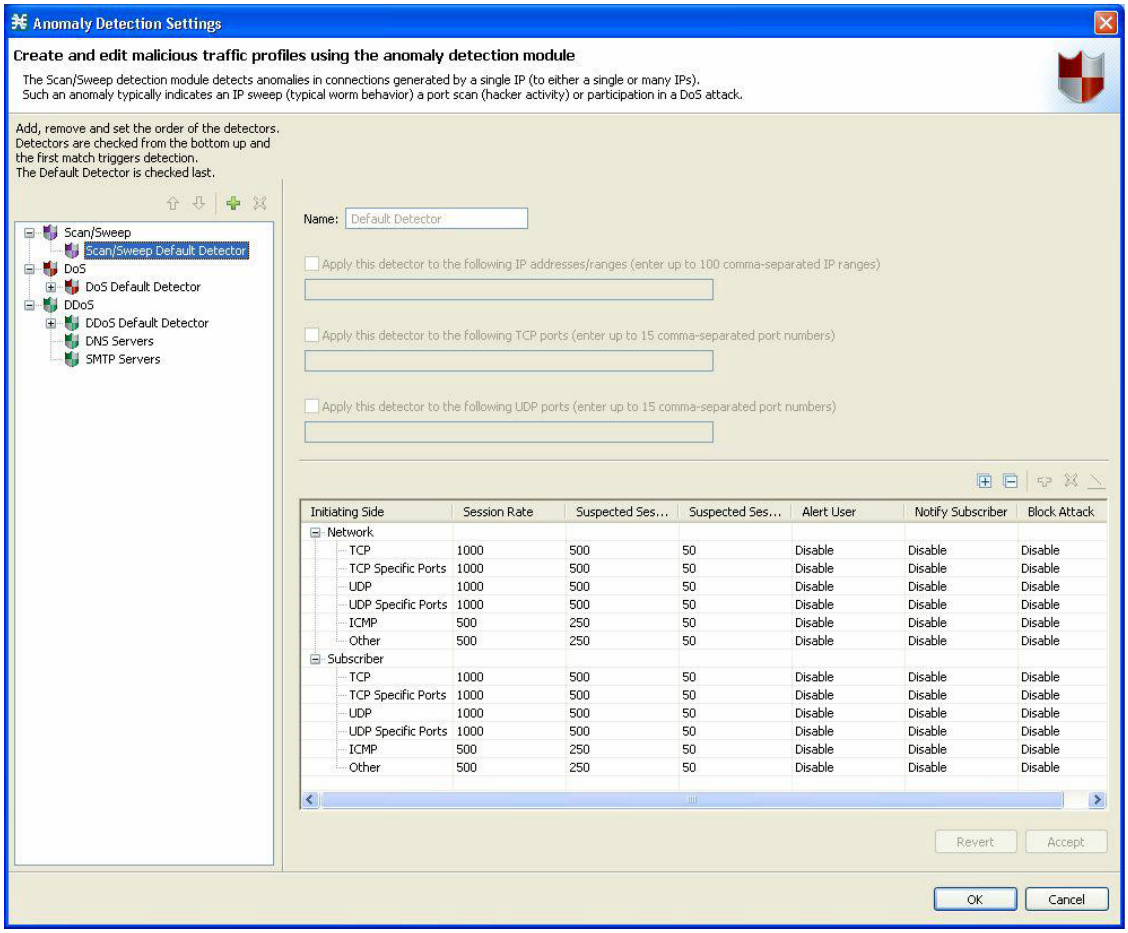

Anomaly Detection Settings
Create and edit malicious traffic profiles using the anomaly detection module
The DoS detection module detects anomalies in connections between two IPs.
Such an anomaly typically indicates the one IP is generating a DoS attack on the other one.
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
DNS Servers
SMTP Servers
Name: Default Detector
Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)
Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)
Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)
Initiating Side | Session Rate | Suspected Ses... | Suspected Ses... | Alert User | Notify Subscriber | Block Attack
Network
TCP 100 50 50 Disable Disable Disable
TCP Specific Ports 100 50 50 Disable Disable Disable
UDP 100 50 50 Disable Disable Disable
UDP Specific Ports 100 50 50 Disable Disable Disable
Subscriber
TCP 100 50 50 Disable Disable Disable
TCP Specific Ports 100 50 50 Disable Disable Disable
UDP 100 50 50 Disable Disable Disable
UDP Specific Ports 100 50 50 Disable Disable Disable
Revert
Accept
OK
Cancel
210235

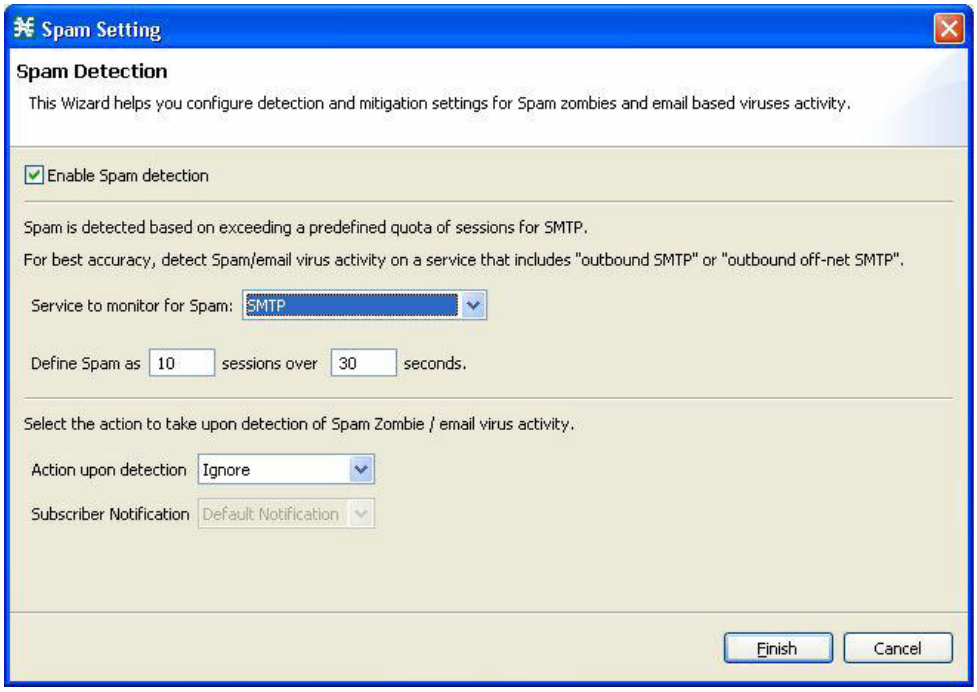

Global DoS Rate
Time Span: 2006-04-06 16:04:44 - 2006-04-09 16:04:44
Sessions per Sec
4,500
4,000
3,500
3,000
2,500
2,000
1,500
1,000
500
0
07-04-2006 04:00
08-04-2006 04:00
09-04-2006 04:00
Date and Time
UDP
TCP
ICMP
210236

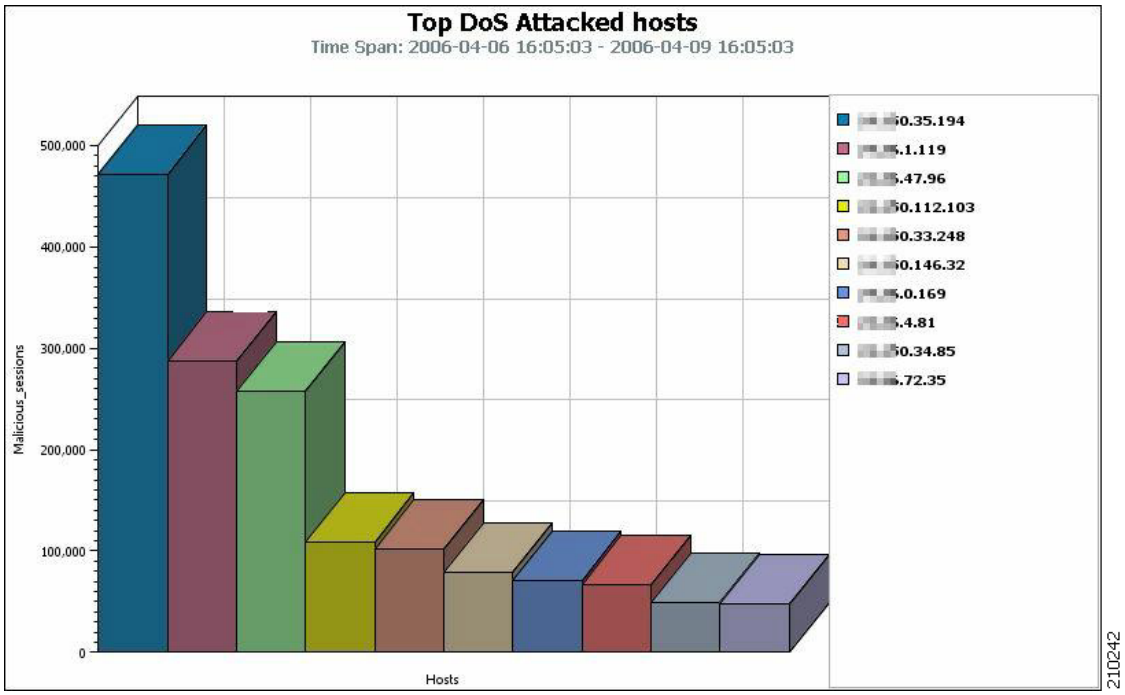

Global Scan or Attack Rate
Time Span: 2006-04-06 16:04:39 - 2006-04-09 16:04:39
Sessions per Sec
1,600
1,400
1,200
1,000
800
600
400
200
0
07-04-2006 04:00
08-04-2006 04:00
09-04-2006 04:00
Date and Time
TCP
UDP
ICMP
210237

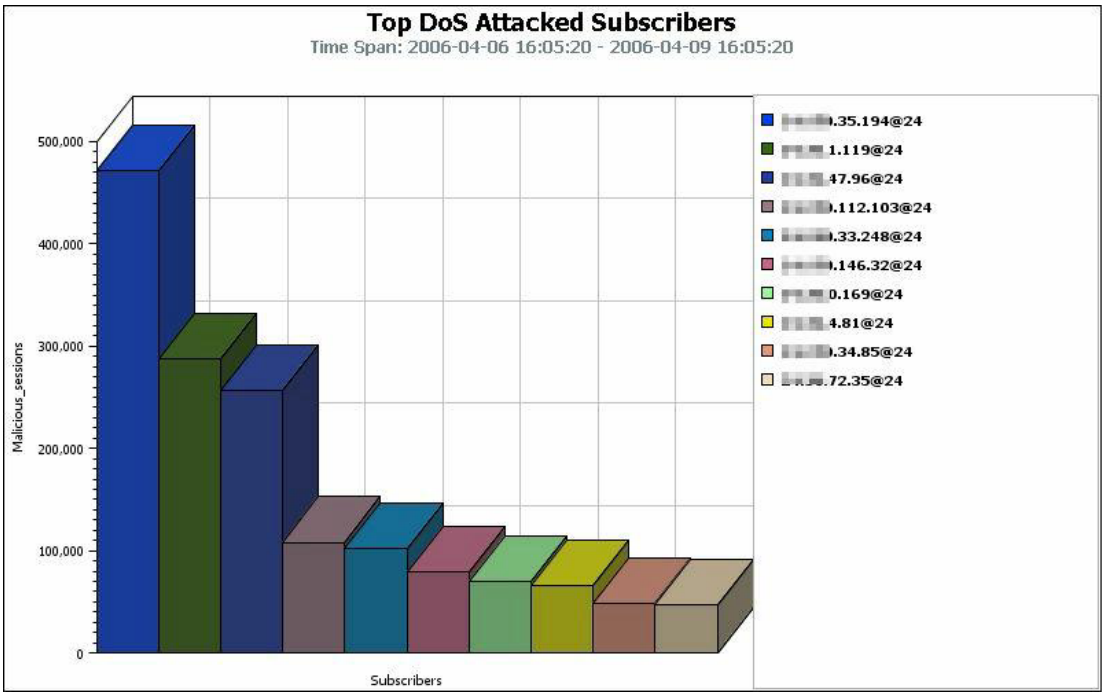

Infected Subscribers
Time Span: 2006-04-06 16:05:09 - 2006-04-09 16:05:09
Infected_Subscriber
Infected Subscribers
40
35
30
25
20
15
10
5
0
07-04-2006 04:00
08-04-2006 04:00
09-04-2006 04:00
Date and Time
210238

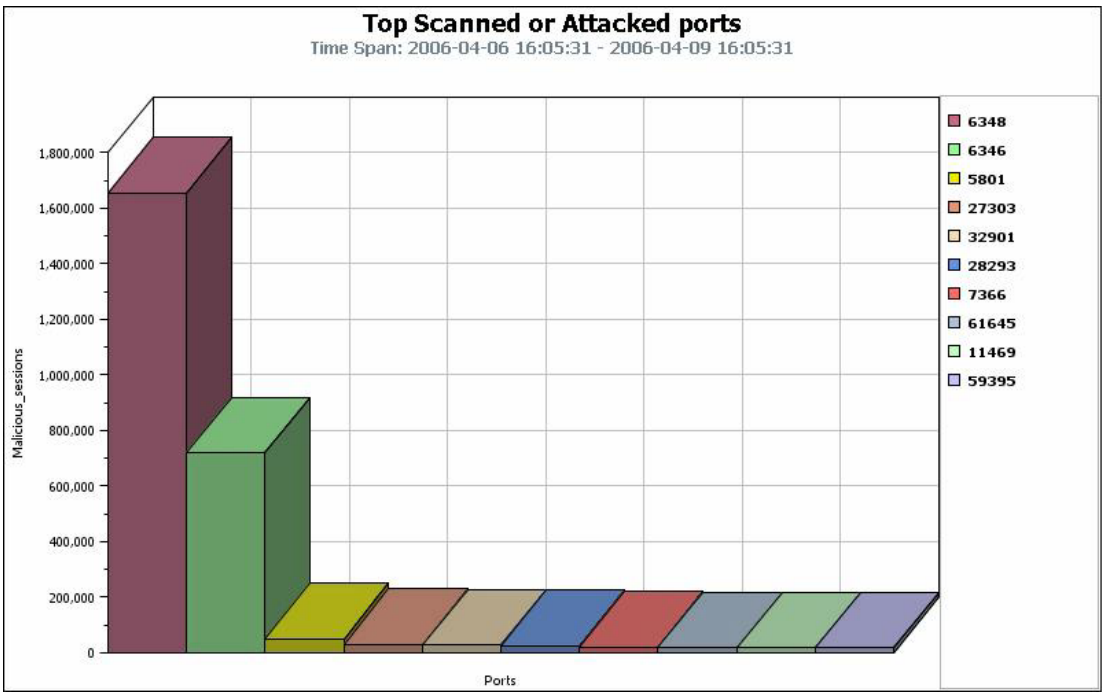

Service Configuration Editor - <new service configuration> - SCAS BB Console
File Edit Tools Network Configuration Window Help
Signature Editor
Reporter
Service Configuration Editor
Network Navigator
*<new service configuration>
Network Traffic : Service Security
Network Traffic
Services
Filtered Traffic
Service Security
Unknown Subscriber Traffic
Controlled Traffic
Default Package
Signature Based Worm Detection
View and configure signatures for worms and other types of malicious traffic.
View Report
View Signatures
Anomaly Based Detection of Malicious Traffic
Define anomaly detection settings and mitigation scheme for worms, DoS/DDoS attacks and VoIP threats.
Enable anomaly detection
View Report
Configure...
Spam Zombies and Email Viruses Detection
Define detection settings and mitigation scheme for Spam Zombies and email based viruses.
View Report
Configure...
Console
Console
Report Only
210239

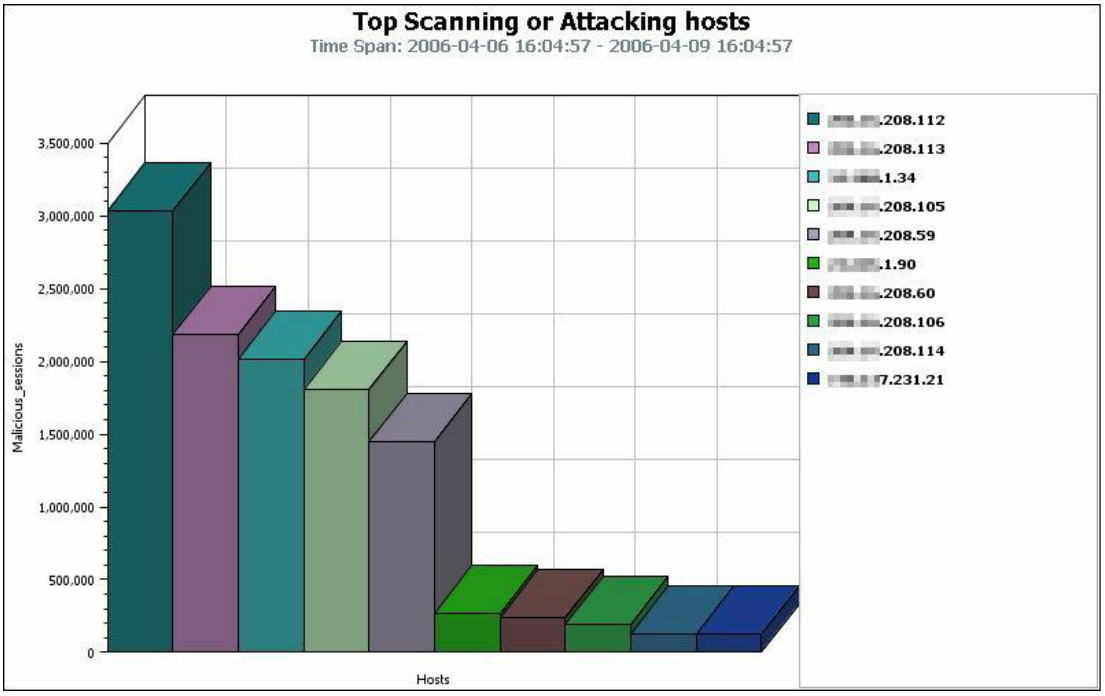

Anomaly Detection Settings
Create and edit malicious traffic profiles using the anomaly detection module
The Scan/Sweep detection module detects anomalies in connections generated by a single IP (to either a single or many IPs).
Such an anomaly typically indicates an IP sweep (typical worm behavior) a port scan (hacker activity) or participation in a DoS attack.
Add, remove and set the order of the detectors.
Detectors are checked from the bottom up and
the first match triggers detection.
The Default Detector is checked last.
Scan/Sweep
Scan/Sweep Default Detector
DoS
DoS Default Detector
DDoS
DDoS Default Detector
DNS Servers
SMTP Servers
Name: Default Detector
Apply this detector to the following IP addresses/ranges (enter up to 100 comma-separated IP ranges)
Apply this detector to the following TCP ports (enter up to 15 comma-separated port numbers)
Apply this detector to the following UDP ports (enter up to 15 comma-separated port numbers)
Initiating Side | Session Rate | Suspected Ses... | Suspected Ses... | Alert User | Notify Subscriber | Block Attack
Network
TCP 1000 500 50 Disable Disable Disable
TCP Specific Ports 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific Ports 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Subscriber
TCP 1000 500 50 Disable Disable Disable
TCP Specific Ports 1000 500 50 Disable Disable Disable
UDP 1000 500 50 Disable Disable Disable
UDP Specific Ports 1000 500 50 Disable Disable Disable
ICMP 500 250 50 Disable Disable Disable
Other 500 250 50 Disable Disable Disable
Revert
Accept
OK
Cancel
210240

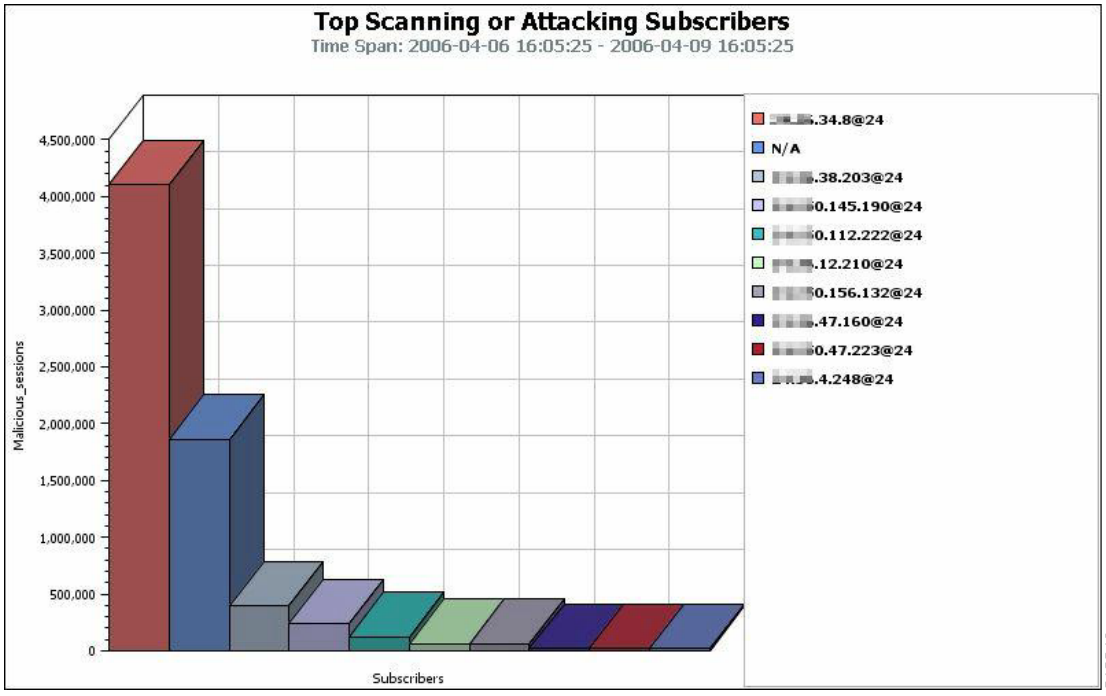

Spam Setting
Spam Detection
This Wizard helps you configure detection and mitigation settings for Spam zombies and email based viruses activity.
Enable Spam detection
Spam is detected based on exceeding a predefined quota of sessions for SMTP.
For best accuracy, detect Spam/email virus activity on a service that includes "outbound SMTP" or "outbound off-net SMTP".
Service to monitor for Spam: SMTP
Define Spam as 10 sessions over 30 seconds.
Select the action to take upon detection of Spam Zombie / email virus activity.
Action upon detection Ignore
Subscriber Notification Default Notification
Finish
Cancel
210241

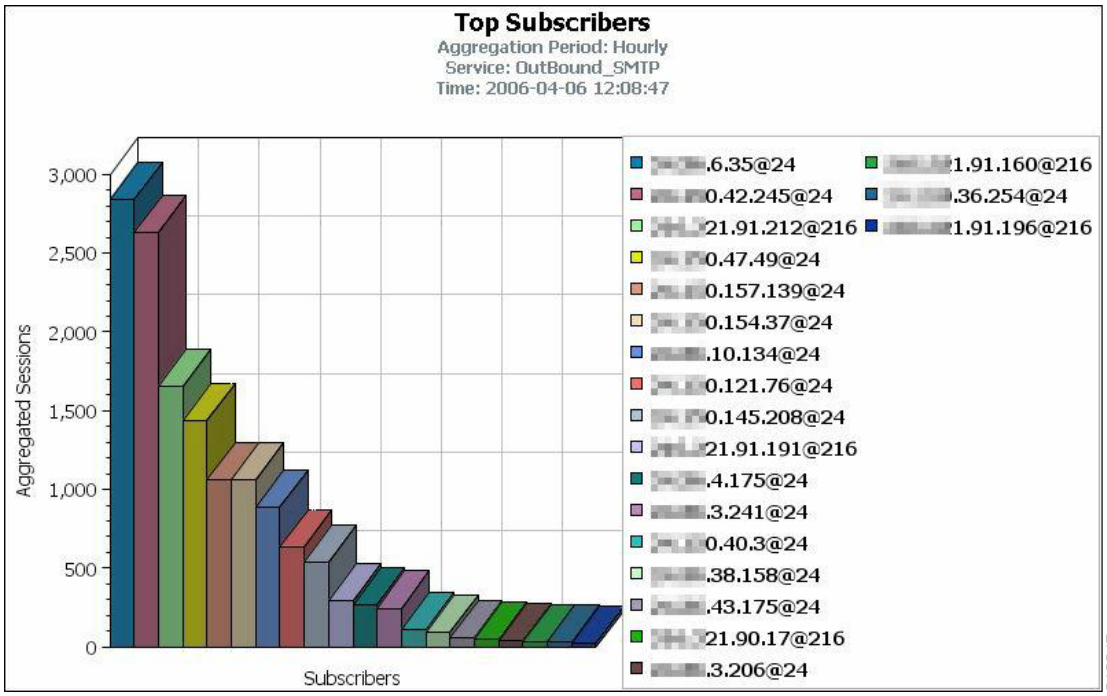

Top DoS Attacked hosts
Time Span: 2006-04-06 16:05:03 - 2006-04-09 16:05:03
500,000
400,000
300,000
200,000
100,000
0
Malicious_sessions
Hosts
210242


Top DoS Attacked Subscribers
Time Span: 2006-04-06 16:05:20 - 2006-04-09 16:05:20
500,000
400,000
300,000
200,000
100,000
0
Malicious_sessions
Subscribers
.35.194@24
1.119@24
47.96@24
.112.103@24
.33.248@24
.146.32@24
0.169@24
4.81@24
.34.85@24
72.35@24
210243


Top Scanned or Attacked ports
Time Span: 2006-04-06 16:05:31 - 2006-04-09 16:05:31
1,800,000
1,600,000
1,400,000
1,200,000
1,000,000
800,000
600,000
400,000
200,000
0
Malicious_sessions
Ports
6348
6346
5801
27303
32901
28293
7366
61645
11469
59395
210244


Top Scanning or Attacking hosts
Time Span: 2006-04-06 16:04:57 - 2006-04-09 16:04:57
Malicious_sessions
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Hosts
.208.112
.208.113
1.34
.208.105
.208.59
1.90
.208.60
.208.106
.208.114
7.231.21
210245


Top Scanning or Attacking Subscribers
Time Span: 2006-04-06 16:05:25 - 2006-04-09 16:05:25
Malicious_sessions
4,500,000
4,000,000
3,500,000
3,000,000
2,500,000
2,000,000
1,500,000
1,000,000
500,000
0
Subscribers
.34.8@24
N/A
.38.203@24
0.145.190@24
0.112.222@24
.12.210@24
0.156.132@24
.47.160@24
0.47.223@24
.4.248@24
210246



210387.tif

210388.tif

210389.tif

210390.tif

210391.tif

210392.tif

210393.tif

210394.tif

210395.tif

210396.tif

210397.tif

210398.tif

210399.tif

210400.tif

210401.tif

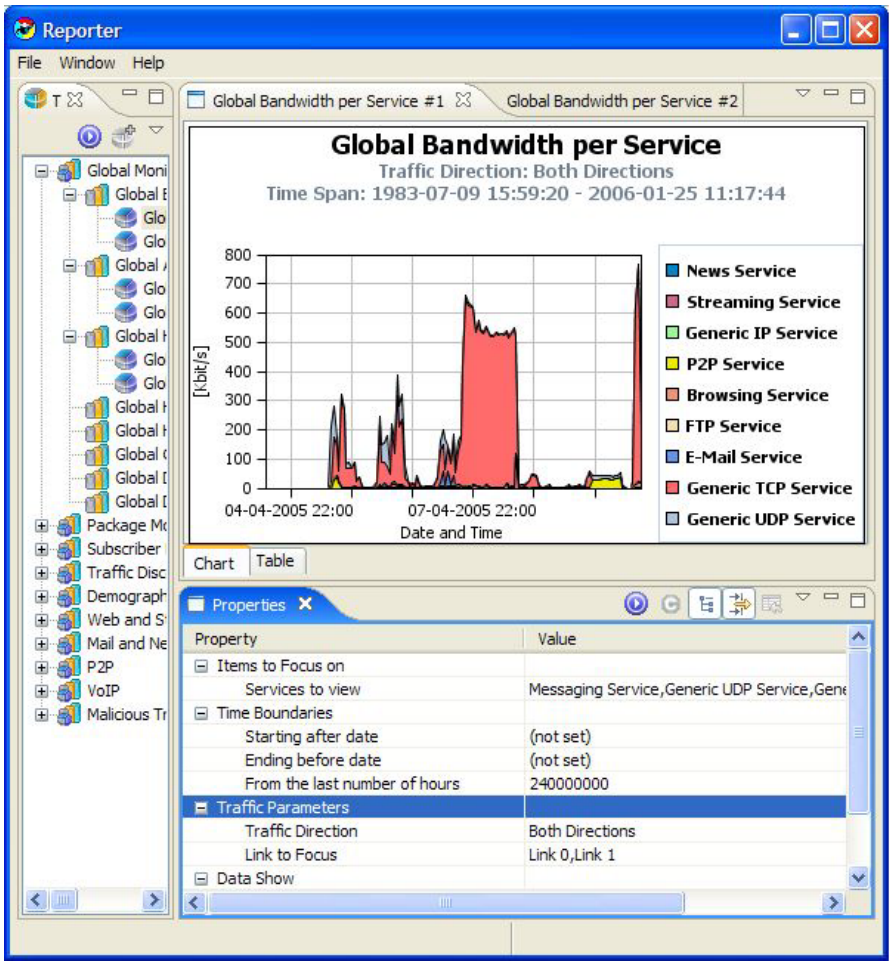
210402.tif

210403.tif

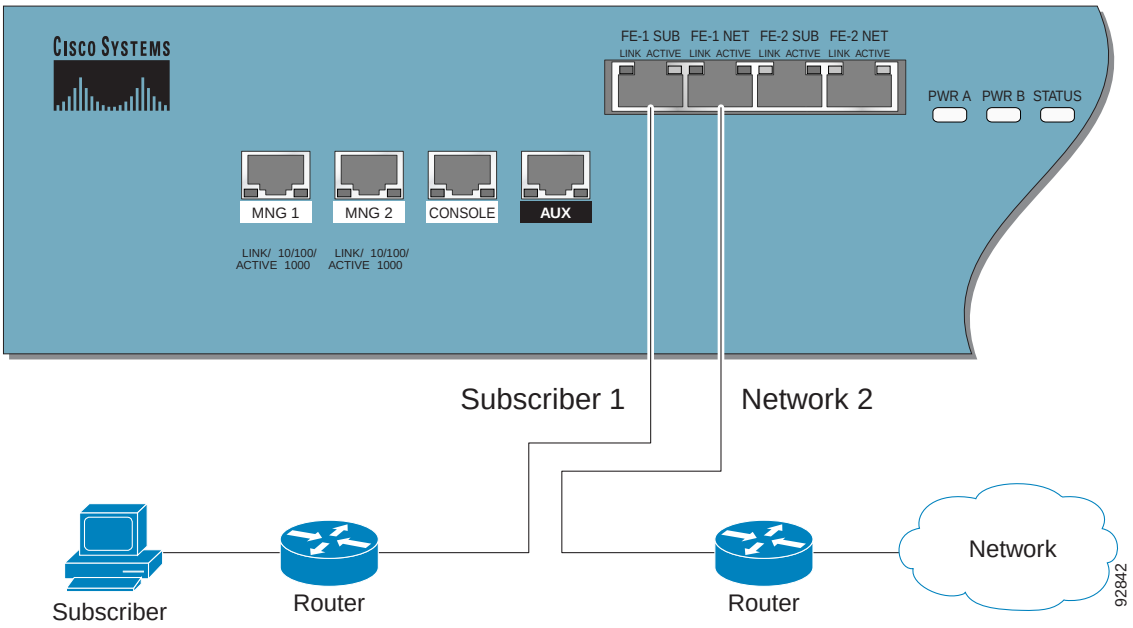
210404.tif

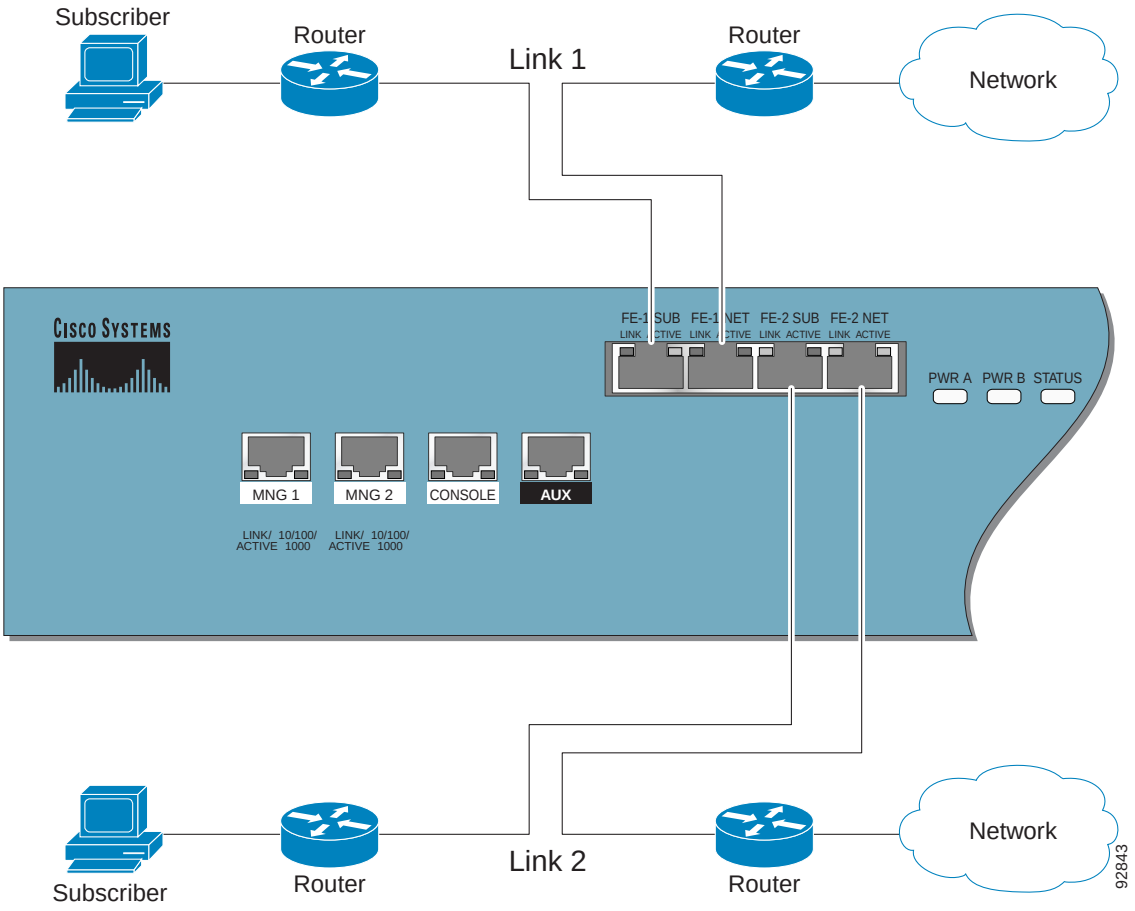
210405.tif

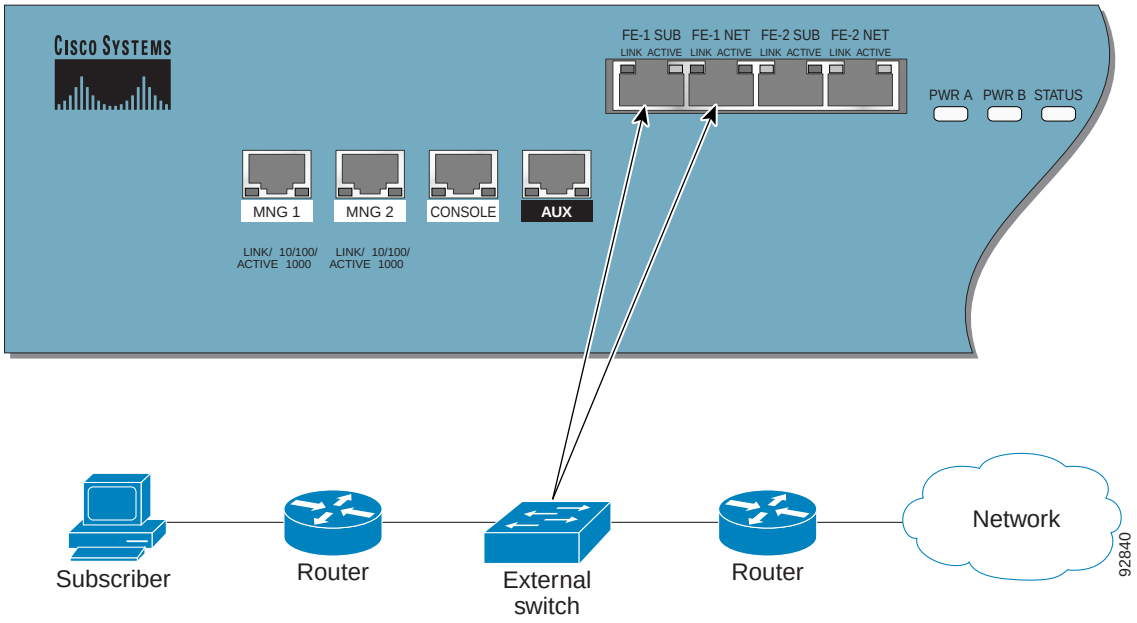
210406.tif

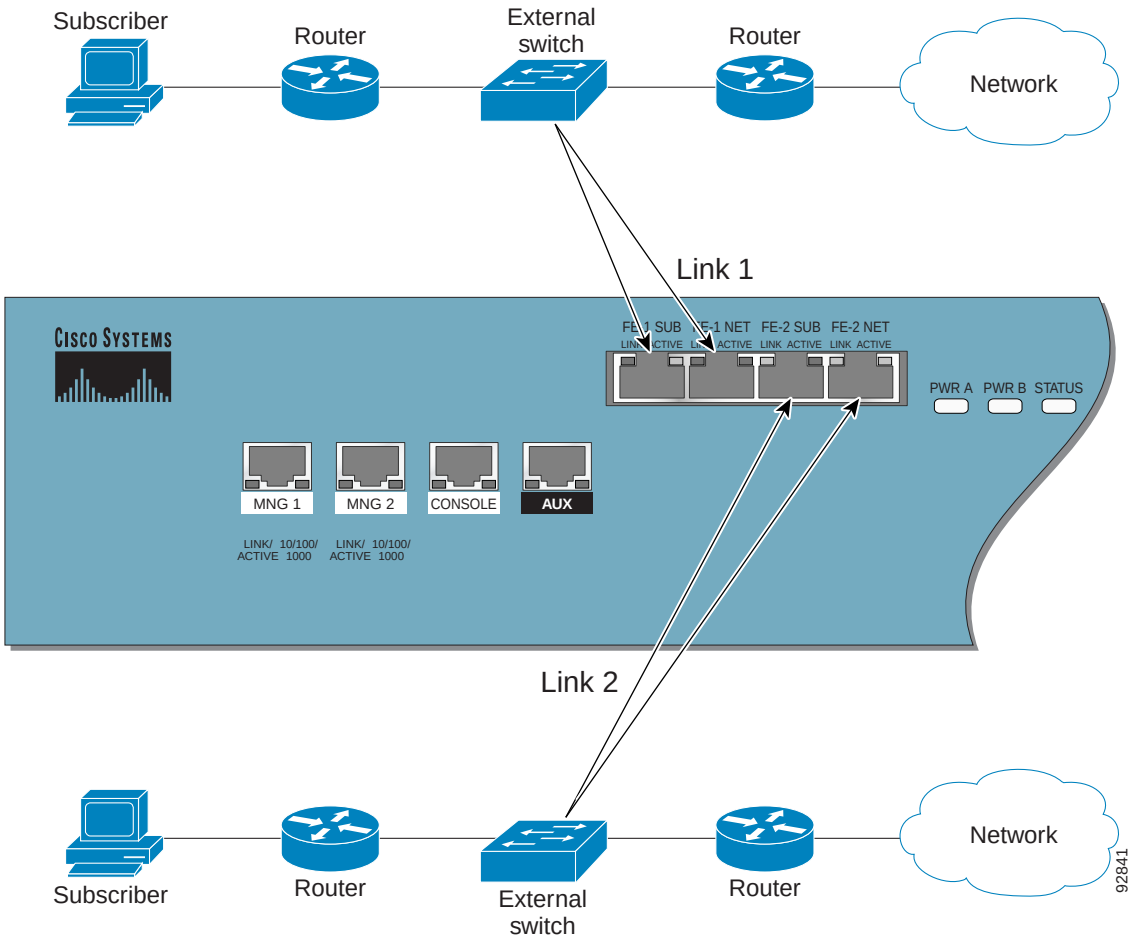

Reporter
File Window Help
Global Bandwidth per Service #1
Global Bandwidth per Service #2
Global Bandwidth per Service
Traffic Direction: Both Directions
Time Span: 1983-07-09 15:59:20 - 2006-01-25 11:17:44
[kbit/s]
800
700
600
500
400
300
200
100
0
04-04-2005 22:00
07-04-2005 22:00
Date and Time
News Service
Streaming Service
Generic IP Service
P2P Service
Browsing Service
FTP Service
E-Mail Service
Generic TCP Service
Generic UDP Service
Chart
Table
Properties
Property
Value
Items to Focus on
Services to view
Messaging Service,Generic UDP Service,Gene
Time Boundaries
Starting after date
(not set)
Ending before date
(not set)
From the last number of hours
240000000
Traffic Parameters
Traffic Direction
Both Directions
Link to Focus
Link 0,Link 1
Data Show
Global Moni
Package Mc
Subscriber
Traffic Disc
Demograph
Web and S
Mail and Ne
P2P
VoIP
Malicious Tr
210579

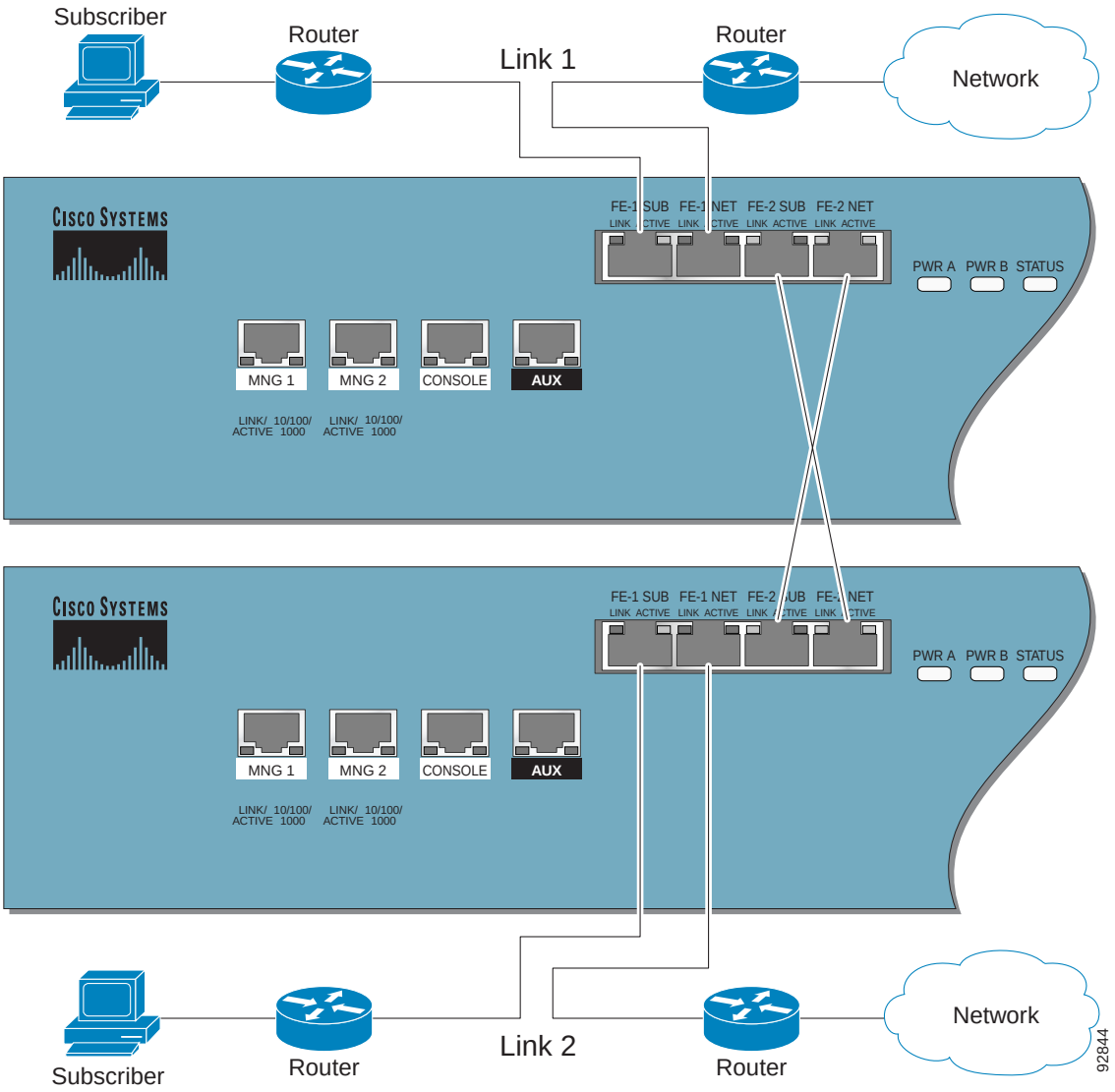

Executing Global Ban...W Per Serv

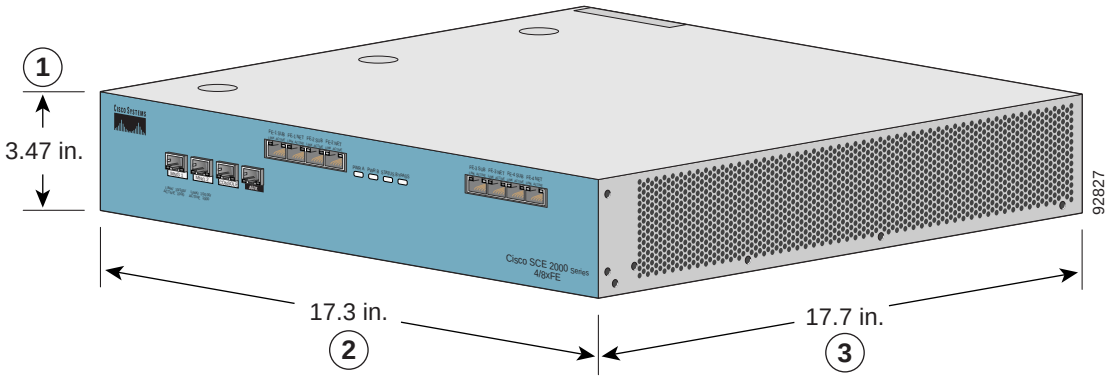

Cisco Systems
FE-1 SUB
FE-1 NET
FE-2 SUB
FE-2 NET
LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/ 1000
LINK/ ACTIVE 10/100/ 1000
Subscriber 1
Network 2
Subscriber
Router
Router
Network
92842

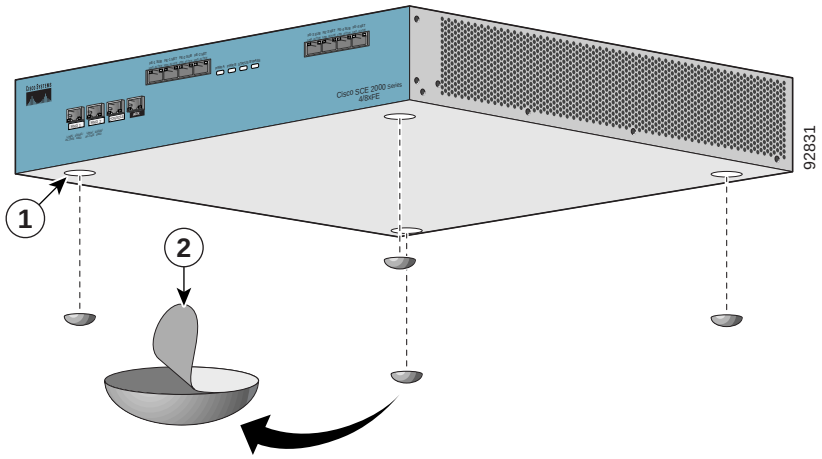

Subscriber
Router
Link 1
Router
Network
CISCO SYSTEMS
FE-1 SUB LINK ACTIVE
FE-1 NET LINK ACTIVE
FE-2 SUB LINK ACTIVE
FE-2 NET LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/1000
LINK/ ACTIVE 10/100/1000
Subscriber
Router
Link 2
Router
Network
92843

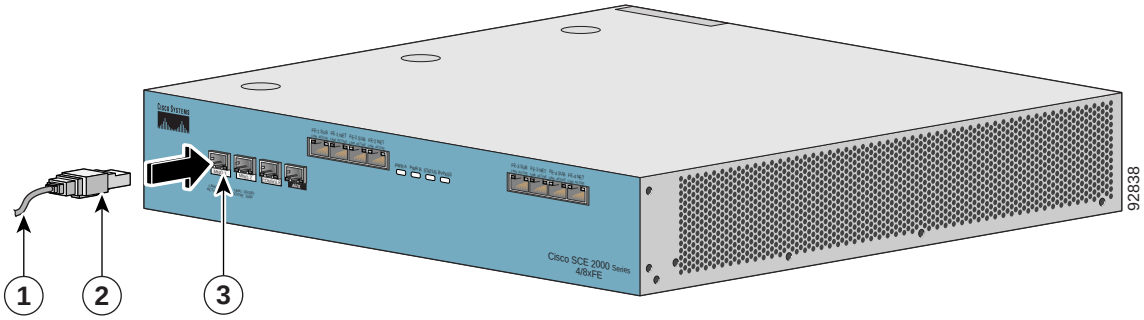

CISCO SYSTEMS
FE-1 SUB LINK ACTIVE
FE-1 NET LINK ACTIVE
FE-2 SUB LINK ACTIVE
FE-2 NET LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/1000
LINK/ ACTIVE 10/100/1000
Subscriber
Router
External switch
Router
Network
92840

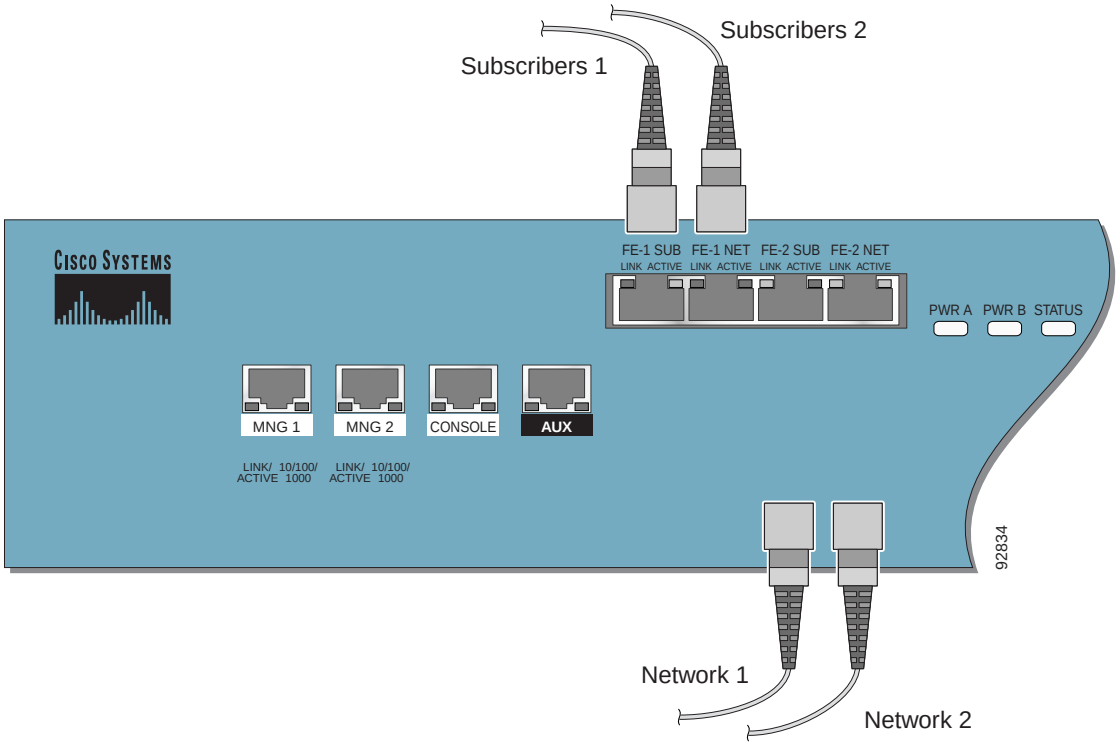

Subscriber
Router
External switch
Router
Network
Link 1
Cisco Systems
FE-1 SUB
FE-1 NET
FE-2 SUB
FE-2 NET
LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/ 1000
LINK/ ACTIVE 10/100/ 1000
Link 2
Subscriber
Router
External switch
Router
Network
92841

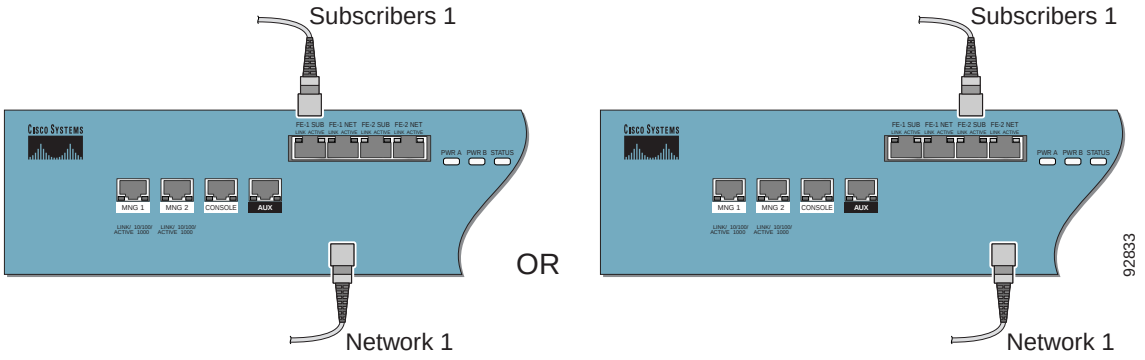

Subscriber
Router
Link 1
Router
Network
Cisco Systems
FE-1 SUB LINK ACTIVE
FE-1 NET LINK ACTIVE
FE-2 SUB LINK ACTIVE
FE-2 NET LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/ 1000
LINK/ ACTIVE 10/100/ 1000
Cisco Systems
FE-1 SUB LINK ACTIVE
FE-1 NET LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/ 1000
LINK/ ACTIVE 10/100/ 1000
Subscriber
Router
Link 2
Router
Network
92844

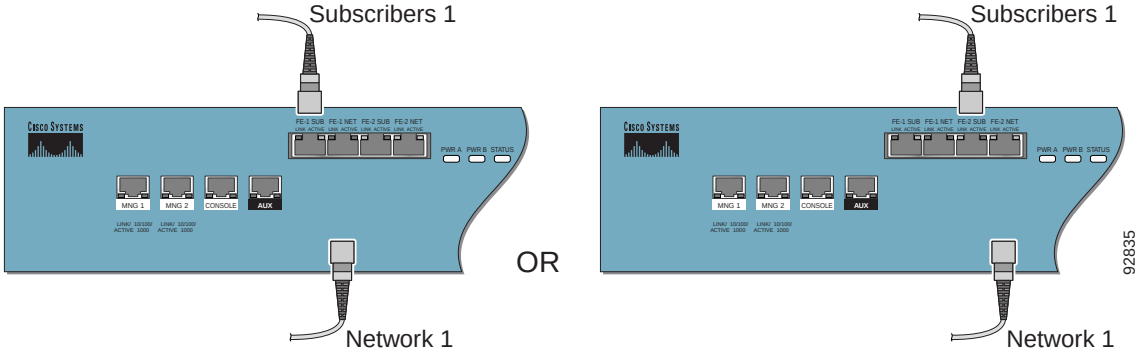

1
3.47 in.
17.3 in.
2
17.7 in.
3
92827

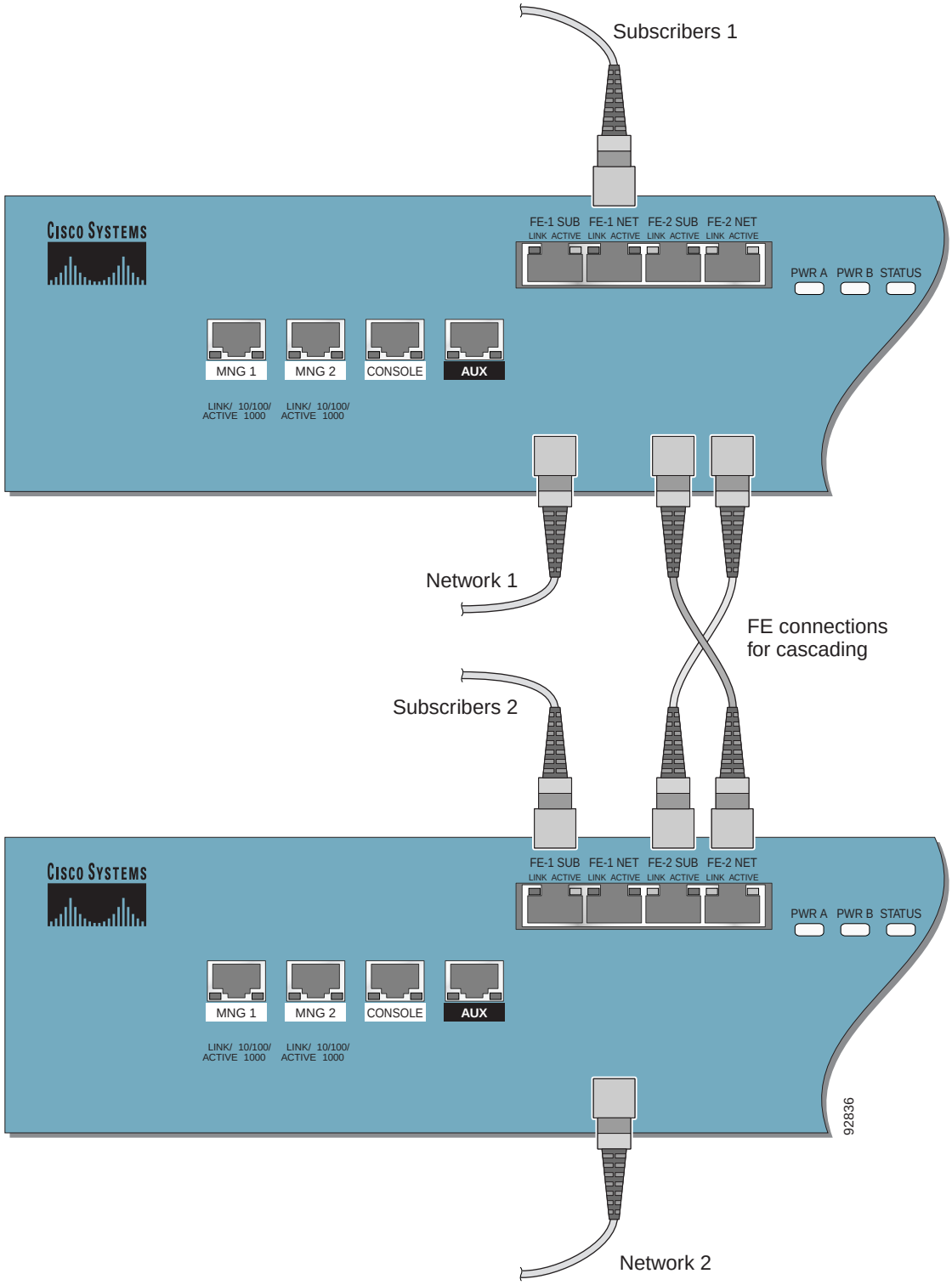

1
2
92831

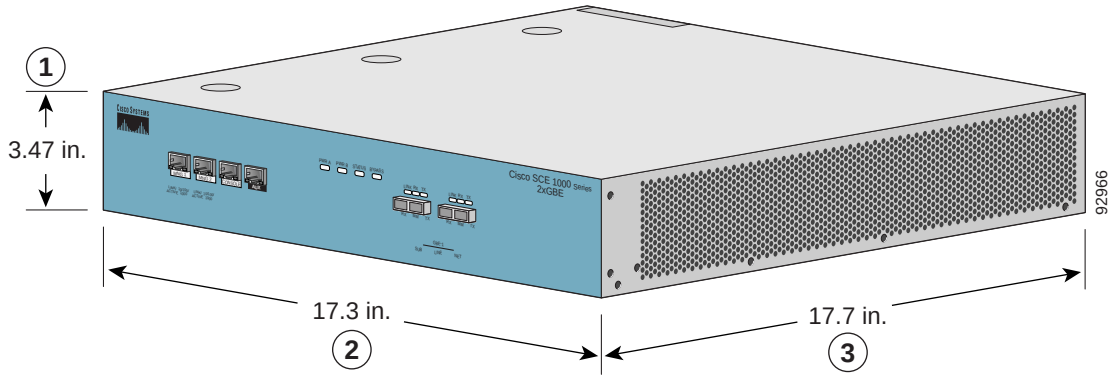

1
2
3
92838

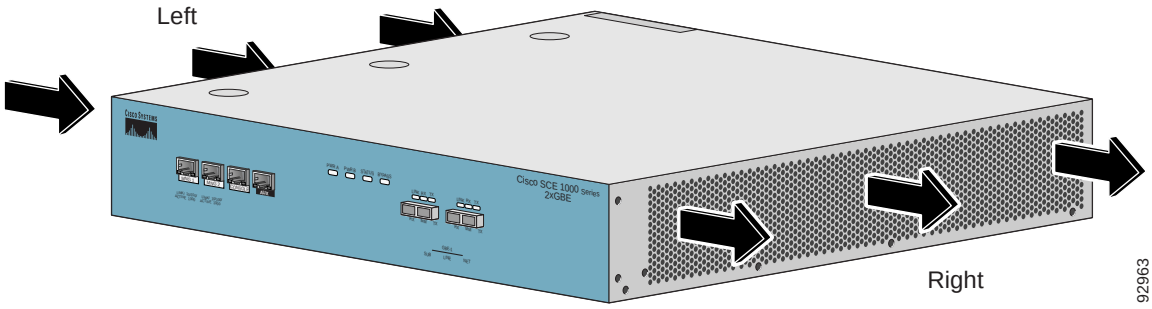

Subscribers 2
Subscribers 1
CISCO SYSTEMS
FE-1 SUB LINK ACTIVE
FE-1 NET LINK ACTIVE
FE-2 SUB LINK ACTIVE
FE-2 NET LINK ACTIVE
PWR A
PWR B
STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ ACTIVE 10/100/ 1000
LINK/ ACTIVE 10/100/ 1000
92834
Network 1
Network 2

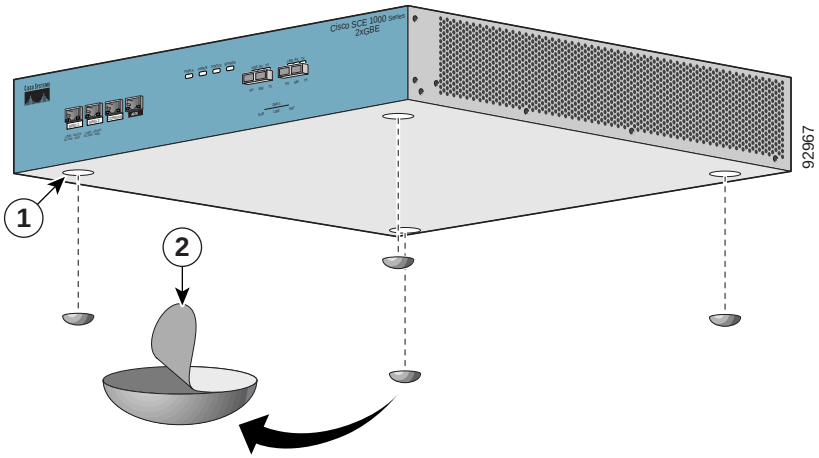

Subscribers 1
Network 1
OR
Subscribers 1
Network 1
92833

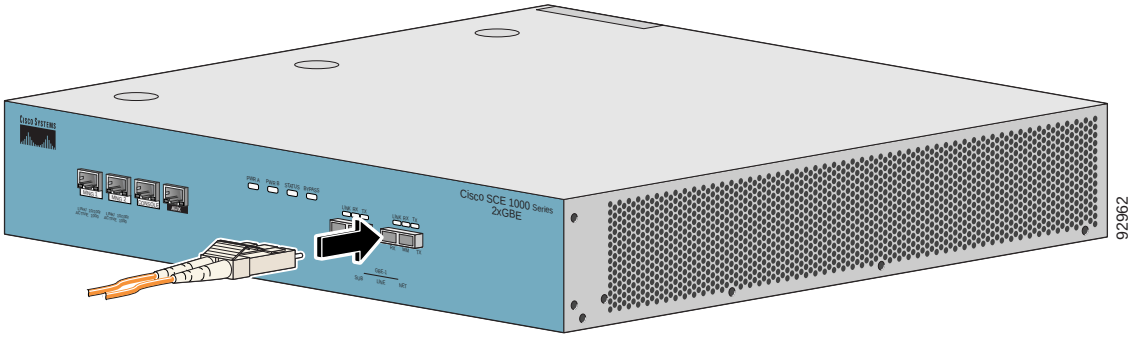

Subscribers 1
Network 1
OR
Subscribers 1
Network 1
92835


Subscribers 1
CISCO SYSTEMS
FE-1 SUB FE-1 NET FE-2 SUB FE-2 NET
LINK ACTIVE LINK ACTIVE LINK ACTIVE LINK ACTIVE
PWR A PWR B STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ 10/100/
ACTIVE 1000
LINK/ 10/100/
ACTIVE 1000
Network 1
FE connections
for cascading
Subscribers 2
CISCO SYSTEMS
FE-1 SUB FE-1 NET FE-2 SUB FE-2 NET
LINK ACTIVE LINK ACTIVE LINK ACTIVE LINK ACTIVE
PWR A PWR B STATUS
MNG 1
MNG 2
CONSOLE
AUX
LINK/ 10/100/
ACTIVE 1000
LINK/ 10/100/
ACTIVE 1000
92836
Network 2


1
3.47 in.
17.3 in.
2
17.7 in.
3
92966


Left
Right
92963


1
2
92967


Cisco SCE 1000 Series
2xGBE
92962