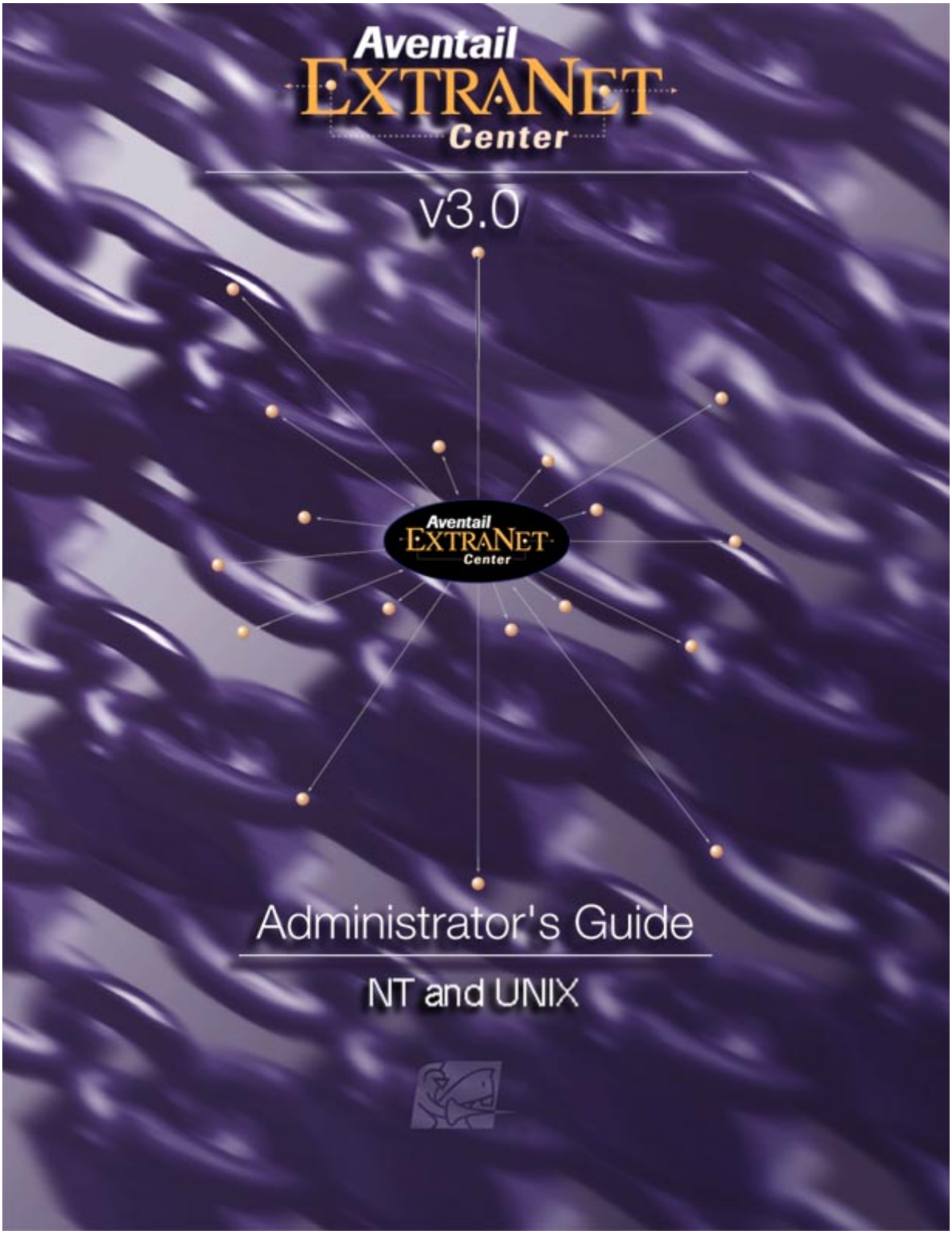

Aventail
EXTRANET
Center
v3.0
Aventail
EXTRANET
Center
Administrator's Guide
NT and UNIX

Table of Contents

AVENTAIL EXTRANET CENTER QUICK START GUIDE

POLICY CONSOLE

Petitioner Apple Inc. - Ex. 1011, p. i

Petitioner Apple Inc. - Ex. 1011, p. ii

CONFIGURATION FILE FORMAT

Petitioner Apple Inc. - Ex. 1011, p. iii

Aventail ExtraNet Server Quick Start Guide

Welcome to the Aventail ExtraNet Server Quick Start Guide.

Aventail ExtraNet Server is the server component of the Aventail ExtraNet Center, a client/server solution for management of sophisticated extranets. Setup of the Aventail ExtraNet Center requires that installation on both a server and multiple client machines. Setup of the Aventail ExtraNet Server consists of installing several components.

AVENTAIL EXTRANET CENTER COMPONENTS

The following are the components of the Aventail ExtraNet Center.

- **Aventail ExtraNet Server:** The primary component of Aventail ExtraNet Center is the ExtraNet Server. This is a SOCKS v5 proxy server that manages the authentication of users and processes all of the connection requests. Aventail ExtraNet Server can manage traffic for both incoming (external users attempting to reach internal network resources) and outgoing (internal users attempting to reach external network resources) network traffic.
- **Aventail Policy Console:** The Aventail Policy Console is the graphical administrative tool for creating, viewing and managing the policies for your extranet. It can also be used for starting and stopping the ExtraNet Server as well as viewing log and license files.

  The Policy Console provides a graphical front-end for the configuration file that the Aventail ExtraNet Server uses. The Policy Console can be run locally on the machine that the ExtraNet Server is installed on or remotely to manage a server that resides on another machine. When the Policy Console is being run remotely, it will establish a secure LAN, WAN or Internet connection via the Management Server (see below). A remote Policy Console running on a Windows NT machine can configure a UNIX Aventail ExtraNet Server and vice versa.
- **Aventail Management Server:** The Aventail Management Server is an optional service that allows administrators to remotely manage an ExtraNet Server. The Management Server and Policy Console communicate via a secure, encrypted connection.

  The Management Server must be installed on the same machine as the ExtraNet Server.
- **Aventail Management Server Config Tool:** The Aventail Management Server Config Tool is the administrative utility that establishes a policy specific to the Management Server. This policy will determine which administrators can manage the ExtraNet Server, how they must authenticate and which network interfaces the server will accept traffic from. The policy also defines the specific directories that can be browsed remotely.
- **Aventail Connect:** Aventail Connect is the client component of the Aventail ExtraNet Center solution.

Petitioner Apple Inc. - Ex. 1011, p. 5

AVENTAIL EXTRANET SERVER INSTALLATION

The following instructions will get the Aventail ExtraNet Server up and running in a very basic configuration.

Windows NT

The general Aventail ExtraNet Server configuration will require encrypted sessions only and force all users to authenticate against the accounts in the Windows NT Server username/password database. This configuration provides unrestricted access for both outbound and inbound traffic. A sample X.509 certificate is supplied and configured during installation and should be used for non-secure testing purposes only.

Instructions on tightening access controls, configuration as a dual-homed server, obtaining "real" digital certificates, configuring the Aventail Management Server, and changing other parameters may be found in the "Aventail ExtraNet Center Administration Guide" located in the "`\docs`" directory.

1. **Installation:** Run `setup.exe` from the Aventail ExtraNet Center directory of the CD-ROM or run the downloaded distribution file.
2. **License File:** Copy the `aventail.alf` license file into the `C:\Aventail\etc` directory. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Run the Policy Console:** Start | Programs | Aventail ExtraNet Center | Policy Console.
4. **Modify Default Configuration File:** From the Access Control tab, click on the red box to the left of the Action column to change the rule from Deny to Permit. The box color will turn green and the text under the Action column will change to Permit.
5. **Start the Aventail ExtraNet Server**:
   - From Policy Console menu bar, select File | Save.
   - Select Services | Configure.
   - Select "Aventail ExtraNet Server."
   - Click "Start."

UNIX

The general configuration will require encrypted sessions only and force all users to authenticate against the accounts in the UNIX "`/etc/passwd`" file. This configuration provides unrestricted access for both outbound and inbound traffic. A sample X.509 certificate is supplied and configured during installation and should be used for non-secure testing purposes only.

Instructions on tightening access controls, configuration as a dual-homed server, obtaining "real" digital certificates, configuring the Aventail Management Server, and changing other parameters may be found in the "Aventail ExtraNet Center Administrator's Guide" located in the "`/docs`" directory.

1. **Installation:** Run the `install.sh` script from the Aventail ExtraNet Center directory of the CD-ROM or install the downloaded distribution file.

Petitioner Apple Inc. - Ex. 1011, p. 6

NOTE: *This will install into the default directory,* `/usr/local/aventail`*. If you wish to install into a different location, specify by executing the* `install.sh` *script with the "prefix" switch. For example:*
`install.sh --prefix=/<install directory>/`
where `<install directory>` *is the location to install.*

2. **License File:** Copy the `aventail.alf` license file into the `/etc` directory of the installation root. The default is `/usr/local/aventail/etc`. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Run the Policy Console:** At the command line, type:
   `<install directory>/bin/apc`
4. **Modify Default Configuration:** File From the Access Control tab, click on the red box to the left of the Action column to change the rule from Deny to Permit. The box color will turn green and the text under the Action column will change to Permit.
5. **Start the Aventail ExtraNet Server**:
   - From the Policy Console menu bar, select File | Save.
   - Select Services | Configure.
   - Select "Aventail ExtraNet Server."
   - Click "Start."

     - OR -

     From the command line, type:

     `<install directory>/bin/socks5`

     `-s for log to stderr -p <port>` for port values other than 1080

CLIENT INSTALLATION

These installation steps will get the client component of Aventail ExtraNet Center, Aventail Connect, up and running in a basic configuration. Instructions covering advanced configuration options, public certificates, and troubleshooting may be found in the "Aventail Connect Administrator's Guide" and in the online Help.

NOTE: *Leave all settings not described below as DEFAULTS.*

1. **Installation:** Run `setup.exe` from the Aventail Connect directory of the CD-ROM or run the downloaded distribution file.
2. **License File:** Copy the `aventail.alf` license file into the `C:\Program Files\Aventail\Connect` directory. (The license file is obtained automatically via email after downloading or provided on diskette following purchase.)
3. **Create a Configuration File**:
   - Select Programs | Aventail Connect | Configuration Tool.
   - Select File | New.

Petitioner Apple Inc. - Ex. 1011, p. 7

4. **Add Server Definition**:
   - From the Servers tab, click Add.
   - Type in Alias name =”Aventail ExtraNet Server.”
   - Hostname or IP address = public DNS hostname or IP address of machine with Aventail ExtraNet Server installed and running. This host must be reachable by TCP/IP (i.e., ping test).
   - Click OK.
5. **Define Destinations**:
   - From the Destinations tab, click Add.
   - Type in Alias name = “Private Network.”
   - Select “Network.”
   - Domain Name = <internal DNS Domain name for private network>.
   - Select “Subnet.”
   - Enter network IP Address/Subnet mask.
   - Click OK.
6. **Specify Redirection Rules**:
   - From the Redirection Rules tab, click Add.
   - Select Destination “Private Network.”
   - Select Redirect via “Aventail ExtraNet Server.”
   - Click OK.
   - Click Add.
   - Select Destination “Everything Else.”
   - Do not Redirect.
   - Click OK.
7. **Save Client Configuration File**:
   - From the Config Tool menu bar, select File | Save.
   - Type `aventail.cfg`.
   - Click OK.
   - Select File | Select Make Active.
   - Select File.
   - Select Exit.
8. **Start Aventail Connect**:
   - Start | Programs | Aventail Connect | Connect.
   - Point to new configuration file `aventail.cfg`.
   - Select OK.

Petitioner Apple Inc. - Ex. 1011, p. 8

- Start any TCP application to initiate the connection. The ExtraNet Server or other SOCKS proxy server must be running.

Essential Concepts for Aventail ExtraNet Server Policies

It is important to understand the primary components of the Aventail Policy Manager that are used to build an extranet policy. There are four types of rules that can be used to build an Aventail ExtraNet Server policy:

Access Control Rules

Access control rules define the network resources and services that are accessible to users and groups based on where they are coming from, what day or time it is, how they authenticated, and what their encryption strength is.

The following are the parameters that make up an access control rule:

- **Active/Inactive:** Temporarily disables a rule without having to delete it.
- **Permit/Deny:** Defines whether the rule will permit or deny access based on the criteria selected.
- **Source Networks:** Defines the originating source of the connection for the rule to be applicable.
- **Source Ports:** Defines the originating ports (services) of the connection for the rule to be applicable.
- **Destination Networks:** Defines which network resource(s) the rule will permit or deny access to.
- **Destination Ports:** Defines which services on the Destination Networks can be used by the rule.
- **Users and Groups:** Defines which users and groups the rule applies to.
- **Times:** Defines the times or days the rule is active.
- **Authentication Matching:** Defines the authentication methods to be used for the rule to be applicable.
- **Key Length:** Specifies the encryption strength required for the rule to be applicable.
- **Commands:** Defines the commands that can be used on the specified Destination Networks.

Authentication Rules

Authentication rules define the authentication options available to users or groups based on where they are coming from.

The following are the parameters that make up an authentication rule:

- **Source Networks:** Defines the originating source of the connection for the rule to be applicable.
- **Authentication:** Defines the authentication methods available.

Petitioner Apple Inc. - Ex. 1011, p. 9

Filter Rules

Filters can be applied to network traffic based on the same parameters as an access control rule. This means that you can apply filters on a very granular level, such as only apply them to specific users, traffic between two locations, or during certain times.

- **Filter Type:** Defines which of the loaded (and configured) filters should be used for the rule.
- All other components used for access control rules except permit and deny.

Proxy Chaining Rules

Defines the methods for accessing network destinations located behind other ExtraNet Servers.

- **Destination Networks:** Specifies which network resources the rule will permit or deny access to.
- **Proxy Server:** Specifies the IP address or hostname of the ExtraNet Server that secures the intended network destination.

NOTE: *In order to use proxy chaining, server-to-server authentication methods must be loaded first. Please reference the Aventail ExtraNet Center Administrator's Guide for more information.*

Objects Used to Build Aventail ExtraNet Server Policies

- **Groups:** These can be made up from six different types of user databases: Windows NT, Novell NDS, UNIX passwd, Host, SSL User (X.509), and Single User. Only SSL Users and Single Users can be created and deleted by the administrator. Administrators can select any combination of these six types of users and groups and apply them to rules. Administrators can also select any combination of users and groups and place them in a folder for easy re-use in multiple rules.
- **Source or Destination Networks and Ports:** Network resources can be a host, domain, IP range or subnet. Administrators can select any combination of network resources they have created to use in rules. Administrators can also select any combination of network resources and place them in a folder for easy re-use in multiple rules. Combinations of single ports and port ranges can be applied to source and destination networks to restrict the available services a user can access.
- **Time:** Days of the week and hours during those days or date range for which a rule is applicable.
- **Authentication method:** Available methods include SSL which can use any of the following methods to sub-authenticate users. These methods can also be used individually but will not provide encryption unless used with SSL for sub-authentication. Client certificates can be used in conjunction as well.
  - Username/Password back-ended to Windows NT, NetWare bindery/ NDS, RADIUS, File, Crypt file, UNIX passwd file.

Petitioner Apple Inc. - Ex. 1011, p. 10

  - CRAM back-ended to RADIUS or ACE/Server.
  - CHAP back-ended to RADIUS or file.
- **Key length requirements:** Can be set to any, 40-bit or higher, 56-bit or higher, or 128-bit or higher.
- **Filters:** Available filters include an HTTP filter and an authentication forwarder filter.
- **Commands:** Available commands include any, traceroute, ping, UDP, connect and bind

Petitioner Apple Inc. - Ex. 1011, p. 11

Policy Console

Introduction

The Aventail Policy Console is the graphical administrative tool for creating, viewing, and managing the policies for your extranet. You can also use the Policy Console to start and stop the Aventail ExtraNet Server, or to view log files and license files. The Policy Console provides a graphical front-end for the configuration file that the Aventail ExtraNet Server uses to handle connection requests. There are no major differences between the Windows NT and UNIX Policy Consoles.

The first section of this chapter covers the server settings. These are server-level settings that specify, among other settings, which port to run on, logging, and starting and stopping the Aventail ExtraNet Server. The next section covers the policy part of the server. These various rules consist of access-control rules, authentication rules, filter rules, proxy-chaining rules, and network rules. The Policy Console Tools are covered at the end of this chapter.

For more information on using the Policy Console to manage a remote Aventail ExtraNet Server, refer to the “Management Server” chapter.

Running the Policy Console

On Windows NT:

Start | Programs | Aventail ExtraNet Center | Policy Console

On UNIX:

At the command line, type `<install directory>/bin/apc`

Server Settings

(Add some introductory content here)

SERVER OPTIONS

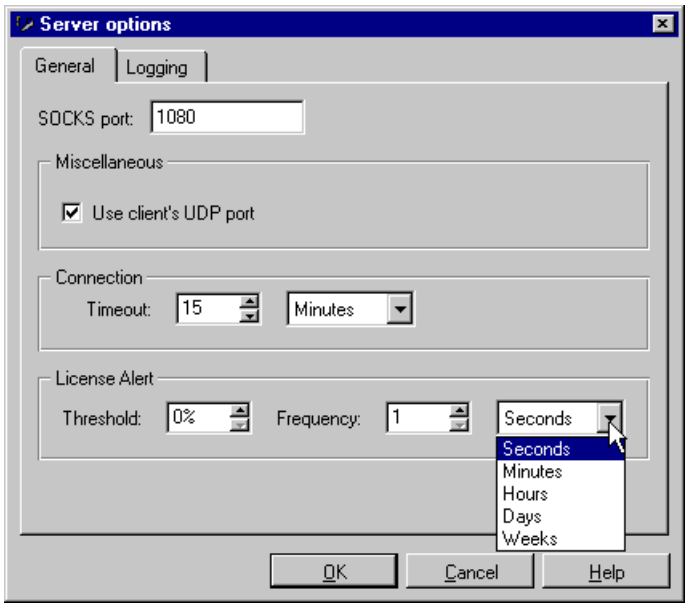
(Add some introductory content here)

General

The Aventail ExtraNet Server requires fundamental licensing and connection information prior to a specific network configuration: how to handle UDP, connection timeouts, concurrent connections, etc.

To open the Server options dialog box, at the Policy Console menu select View | Server Options.

Petitioner Apple Inc. - Ex. 1011, p. 12



SOCKS PORT

This is the port on which the server wil listen for incoming connections. The default is 1080.

USE THE CLIENT'S UDP PORT

Checking this enables support for unknown UDP connections. If enabled, the Aventail ExtraNet Server relays packets from hosts to which it has not previously sent data.

SETTING THE CONNECTION TIMEOUT

Controls the duration of client connections. If there is no activity after a specified period, the client connection will timeout. You can establish a timeout interval of seconds to weeks.

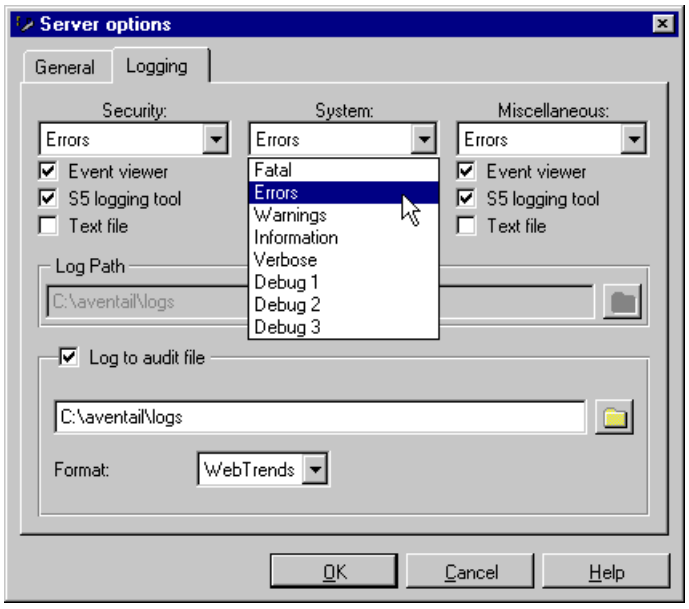
CONFIGURING THE LICENSE ALERT

The license alert will create logging information at predetermined intervals that you are at "X" percentage of your license limit. For example, if you have an Aventail license for 1,000 users and you establish a threshold of 80%, alerts will be sent to your logging at the intervals you determine every time concurrent connections exceed 800.

Logging and Auditing

Logging is an essential part of diagnosing and maintaining server function. With logging you can track user activity, diagnose failed connections, repair system failures, and configure the logging output for Aventail or WebTrends formats.

Petitioner Apple Inc. - Ex. 1011, p. 13



LOGGING

You can select one of three logging methods, one of eight levels of information, and three output options.

LOG METHODS

- Security- Security information will consist of failed authentication attempts and methods. Select the logging level from the drop-down menu and check the desired output option. The default filename is security.log.
- System- System information will point out network problems as they affect the Aventail ExtraNet Server; i.e., low memory, timing out, a SOCKS server crashing, etc. Select the logging level from the drop-down menu and check the desired output option. The default filename is system.log.
- Miscellaneous- Miscellaneous information will consist of everything else not covered by the two prior methods. Select the logging level from the drop-down menu and check the desired output option. The default filename is misc.log.

LOG LEVELS

NOTE: *Processing large amount of information may impact the server's performance for brief periods of time.*

- Fatal- Fatal error information only.
- Error- Critical error information only.
- Warning- Non-critical warning information, as well as Error level information.
- Information- Detailed logging information, including all previous level data.
- Verbose- All previous level data, but less data than Debug 1.

Petitioner Apple Inc. - Ex. 1011, p. 14

- Debug 1, Debug 2, and Debug 3- Debugging programs of increasing debug information. This can be a large amount of data, and should be used only when troubleshooting.

OUTPUT OPTIONS

- Event Viewer- Logging information will output to the Windows NT Event Viewer's Application Log. Note that the server will always log startup information to the Event Viewer, regardless of settings at the Logging tab.
- (S5) Logging Tool (Windows only)- The (S5) Logging Tool is the dynamic logging tool for all (Windows) Aventail ExtraNet Server activity. Start the (S5) Logging Tool via the Tools | Logging Tool menu of the Policy Console.
- Plain-text file- Aventail ExtraNet Server activity information will output to the default logging file, server.log in the Aventail ExtraNet Server installation directory

AUDITING

Enabling this option will direct exportable logging information to the audit log.

OUTPUT FORMATS

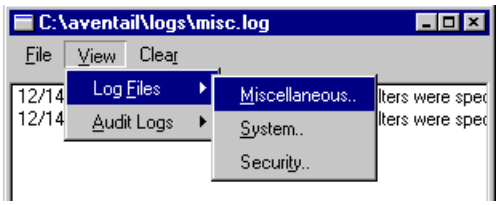
- Aventail- outputs information into the Aventail format.
- Webtrends- Outputs audit log information in the Webtrends format. For more information on Webtrends, contact http://www.webtrends.com.

.

Tips: - To debug the server, use the (S5) Logging Tool (Windows only), and set the Debug level to 3.
- For normal operations, either log to the system log, or log to file.
-To archive traffic through the server, and process reports on it, use the audit log. There are maximum no log settings. However, logging at one of the Debug levels could exhaust server memory.

Petitioner Apple Inc. - Ex. 1011, p. 15

LOG VIEWER



.

NOTE: *At the Policy Console menu, select View | Server Options...to configure the level of information the server will generate for Log files.*

Opening the Log Viewer

Via the View|Log Files... menu command on the Policy Console, you can view the Miscellaneous, System and Security Log files, and the Error, Accounting and Security Audit logs.

NOTE: *Select View|Server Options...|Logging tab to configure the level of information the server will generate for Log files.*

CLEARING LOG AND AUDIT FILES

You can clear the logging or auditing information from a selected file, whether you are viewing it or not. At the Log Viewer, select and:

- the type of log or audit file,
- Current (the file you are viewing), or
- All (files).

RELOADING LOG AND AUDIT FILES

At the Log Viewer, for any log or audit file you are viewing, you can refresh the window with the latest information the server generates for that specific log. You can do this in one of three ways:

- By cursor, select File | Reload at the Log Viewer menu,
- by the keystroke, Ctrl+R, or
- by clicking the Reload button at the bottom of the Log Viewer.

.

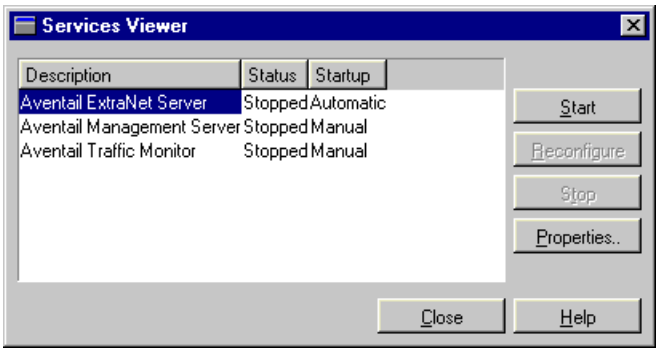
NOTE: *More than one Log Viewer can be opened at one time.*

Petitioner Apple Inc. - Ex. 1011, p. 16

CONFIGURING SERVICES

The Aventail ExtraNet Server has three services (ExtraNet Server, Management Server, and Traffic Monitor) that you can start, stop, and reconfigure. The difference between Start/Stop and Reconfigure is that reconfiguration refreshes your configuration file “on the fly” without having to stop and restart server connections.

This means existing client connections will not be lost and will continue to use the old policy. New incoming connections will use the new policy.



NOTE: *You cannot stop the Management Server remotely.*

Configuring server services

Select Services | Configure... from the Policy Console menu to display the Services Viewer. The Services Viewer displays available services, whether they are running or not, and the buttons for managing the services.

Viewing available services

The window of the Services Viewer contains the description (name) of the service, it status, and its startup configuration (whether automatic, manual or disabled). You can adjust the column width of the Description-Status-Startup bar by dragging the separator bars to the desired width.

Starting a service

Select the service in the Services Viewer and click **Start**.

Changing startup properties

To configure a service to start automatically or manually, or to disable it, select that service in the Service Viewer and click **Properties**. The Properties dialog box will appear. Select one of the three options and click **OK**.

NOTE: *If you want to run the (S5) Logging Tool, you must check the “Interact with desktop” box at the Properties dialog box*

Petitioner Apple Inc. - Ex. 1011, p. 17

Reconfiguring a service

If you've made modifications to your configuration file but are actively using the Aventail ExtraNet Server, you can refresh the configuration file by clicking **Reconfigure**, and the server will use the new configuration file for all new incoming connections, but continue to use the old one for existing connections.

Viewing server status

Select Services | Status from the Policy Console menu to view the activity status of the Aventail ExtraNet Server, Management Server, and Traffic Monitor.

CONNECT TO REMOTE

With proper configuration, the Management Server can establish a connection with another Host, domain, or subnetwork.

Connecting to a remote server

Click Connect on the Policy Console; the Establish Remote Connection dialog box appears. Two text boxes on the dialog box, Host and Port, let you specify the remote server to which you want to connect.

- Host -- enter the IP or host name of the remote ExtraNet
- Port -- enter port on which the Management server is listed. The default port is 2080

After the connection is established the Policy Console is automatically populated with the remote server configuration file. The name of the remote server appears in the titlebar of the Policy console. Browsing in the remote Files, Users, and Groups can now be accomplished from your Policy Console.

To end the remote browsing session, click Disconnect on the Policy Console.

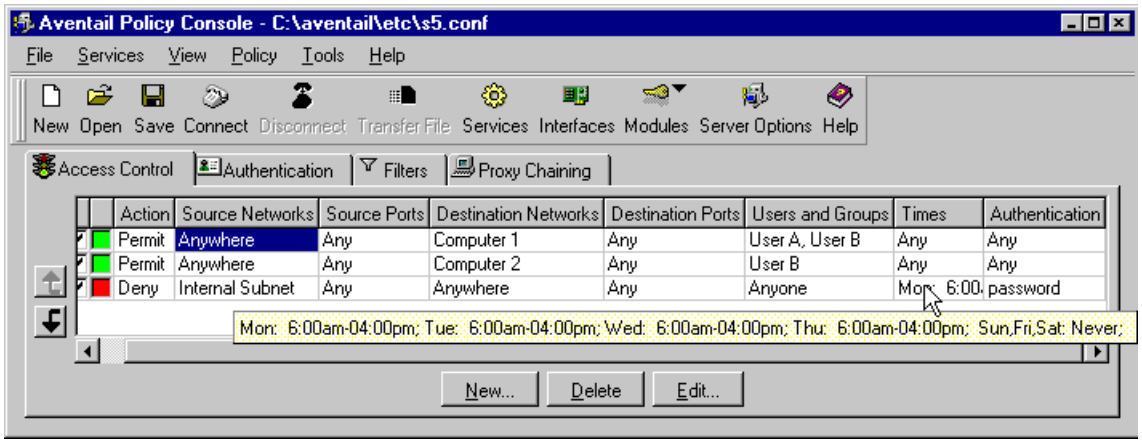
Petitioner Apple Inc. - Ex. 1011, p. 18

Access Control

Access Control rules determine which people and groups can access what machines and services based on where they came from, the time of day, how they authenticated, and encryption strength, etc.

Access Control Tab

The Access Control tab is where you define the rules for specifying which people and groups can access what machines and services. Rule elements include: where they came from, the time of day, how they authenticated, and encryption strength, etc. Rules for machine and services appear on the Access Control tab as row in a grid.



Column headings (definitions)

When you create an access control rule, by either adding or editing, the information appears beneath the column headings of that rule.

How to adjust column width and display cell contents

- To adjust the width of the columns, click on the separator bar between column headings (the cursor will change to arrows), and drag the separator bar, left or right, to the desired width.
- To view the contents of a cell populated with information that runs beyond the cell width, place your cursor in the cell and a ToolTip will display all configured properties for that cell.

You create access control rules with the Access Control Builder. Every access control rule is populated by rule elements located under each column on the grid of the Access Control tab. The server checks client access requests against the access control rules, starting with rule #1, and continues down the list seeking a match between the request and the access requirements of each rule. It does this by comparing any combinations of rule elements. At the first instance of a match, the server stops searching and permits (or denies) access to the client. For this reason you must be sure to create a logical flow to your access rules, from the top down. This is known as rule order.

Petitioner Apple Inc. - Ex. 1011, p. 19

Changing rule order

- To establish the order of a rule, select the entire rule or a cell of that rule. Use the up/down arrows located on the left side of the Access Control tab to move the rule to its new position in rule order.
  -OR-
- Right-click a selected cell of the rule you want to reorder, and select the "move up" or "move down" arrow commands from the shortcut menu.

Adding rules

- On the Access Control tab, click **New...**
  -OR-
- Right-click anywhere in the white area of the Access Control tab grid and select **New...** from the shortcut menu
  -OR-
- Double-click anywhere in the white area of the Access Control tab grid. Any of these actions will open the Access Control Builder.

Editing rules

- On the Access Control tab, select the cell in a rule that you want to modify, and click **Edit...**
  -OR-
- Select the cell in a rule that you want to modify, right-click and select **Edit...** from the shortcut menu.
  -OR-
- Double-click any cell of a rule.
  Any of these actions will open the Access Control Builder at the appropriate tab for the selected cell, with the rule number of the selected cell displayed in the title bar.

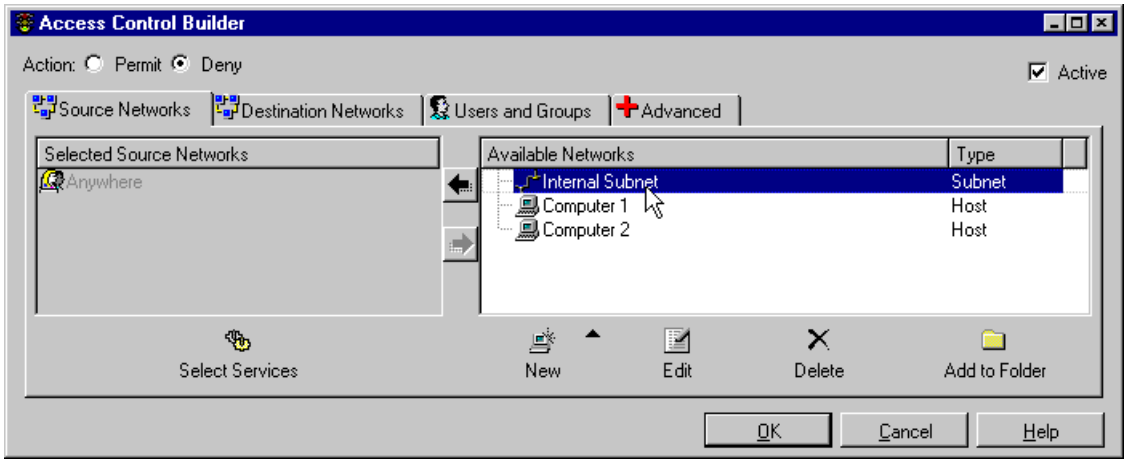
Deleting rules

- On the Access Control tab, select the entire rule or any cell in that rule. Click **Delete**,
  -OR-
- Right-click the selected rule or cell, and select **Delete** from the shortcut menu.

Petitioner Apple Inc. - Ex. 1011, p. 20

ACCESS CONTROL BUILDER

The Access Control Builder gives you access to all the tools necessary to build your access rules: Source and destination networks, users and groups, time-based access limits, authentication matching, key length requirements, commands, etc.



Creating access control rules

Click the appropriate tab on the Access Control Builder to configure that part of the new rule you are creating or existing rule you want to edit:

- Source Networks -- This is where you create or identify your source network for this rule, as well as assign services (ports).
- Destination Networks -- This is where you create or identify your destination network for this rule, and assign services (ports).
- Users and Groups -- You can select a user or group from the Available Users pane or create a new user or group.
- Advanced -- It is at the Advanced tab that you can configure time constraints for the rule, select loaded authentication methods for the rule, require specific key lengths or none, and/or assign network commands (traceroute, ping, UDP, etc.) to the rule.

Assigning a "permit" or "deny" status to a rule

As you create a rule, select either Action: option before you click **OK**. If you select Permit, the server evaluates the rule according to the rule order and offers it to client requests for access to that specific network. If you select deny, the server will evaluate the rule, but not offer it to client requests. You can also assign a permit or deny status to the rule at any time via the Policy Console.

Making a rule active or inactive

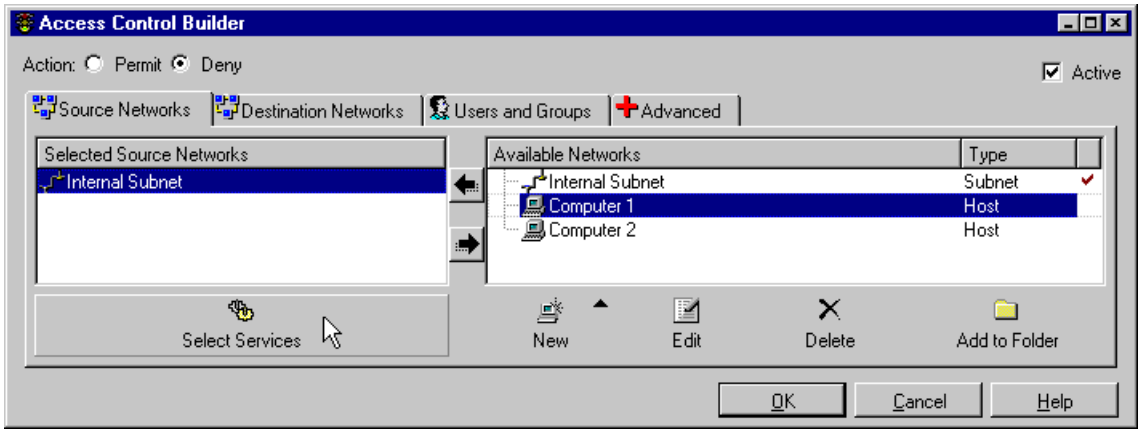
Check the Active: box to make the access control rule active, if it is not. This puts the rule in the rule order queue for server evaluation. If you make the rule inactive, the server will

Petitioner Apple Inc. - Ex. 1011, p. 21

not evaluate the rule or offer it to client requests. You can also make the rule active or inactive at any time via the Policy Console.

Source networks

For your Extranet, traffic starts from a source and travels to a destination, either on the same network, or another network, by way of address protocols. Any host machine on any network has a unique address and can send and receive message traffic, hence it can be both a source and a destination. However, when you need to control message traffic, you must identify source networks and determine where you will allow their message traffic to go. For example, your company (ABC, Inc.) has a relationship with a development team at an XYZ, Inc. office, and all members (groups and users) of that team need to communicate with all members of the product development team from your company. You can assign authentication attributes to the network, create a folder, add the XYZ network to the folder, and select that folder as an active, source network. Once you select the XYZ network as a source network, you can then refine the access rights of anyone coming from that network, e.g., by limiting access to only a specific destination network (Destination Networks tab), during certain times of the day (Advanced tab | Time Editor).



AVAILABLE NETWORKS

The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. You must move the network object to the Selected Source Networks pane to make it a part of an access control rule.

The checkbox located above the right pane indicates whether the access control rule for the selected network is active or disabled.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

Petitioner Apple Inc. - Ex. 1011, p. 22

SELECTED SOURCE NETWORKS

In order to add a source network object to an access control rule (or filter rule), you must move network objects from the right pane into the left pane. The network objects then become Selected Source Networks.

NOTE: *A check mark appears in the Available pane to the right of objects and/or folders to indicate they are active in the Selected pane.*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available Networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Source Networks pane, the Select Services and New tools remain functional, but the Edit, Delete and Add to Folder tools become unusable.

CREATING A NEW (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

- To add a network object to an Available Networks pane, either right-click anywhere in the Policy Console window and select New... from the shortcut menu,
  -OR-
  click **New...**at the Policy Console, then click **New...** in the Access Control Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**. You may also enter Optional Information.

NOTE: *If you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders allow you to group similar network objects under a common name. You can create folders in the Available Networks pane, into or out of which you can move selected networks and groups (only while that folder is in the Available Networks pane). To make that folder an active source network, move it from the Available Networks pane to the Selected Source networks pane, using the arrows, or you can also double-click the network object (folder) to move it back and forth, from one pane to another.

ADDING OBJECTS TO A FOLDER

To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Access Control Builder and select **Add**

Petitioner Apple Inc. - Ex. 1011, p. 23

to from the shortcut menu-OR-Select the objects and click the **Add to Folder** tool. This will open the **Add to Folder** dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the Shift key down as you click the first and last objects of a continuous list, or by holding the Control key to select individual, non-adjacent objects.*

EDITING A SOURCE NETWORK/OBJECT

Right-click a cell under the Source Network column on the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. Either action will open the Access Control Builder at the Source Networks tab. Select the network object you want to edit from the Available pane . Then click the Edit tool on the Access Control Rule. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to the Source Network is global.

DELETING A SOURCE NETWORK/OBJECT

To delete a source network object from an access control rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the access control rules that will be disabled due to the security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

ADDING OR EDITING SERVICES (PORTS)

- You can only add or edit ports for networks or network objects in the Selected Source networks pane. Right-click an object in that pane and select Edit Services from the shortcut menu,
  -OR-
- Select the object in that pane and click Select Services. Either action will open the Selected Services dialog box where you can add or edit network services (ports) to your selected network object.

NOTE: *By allowing only selected services you will restrict the port on which that the client can make the initial access request.*

Destination networks

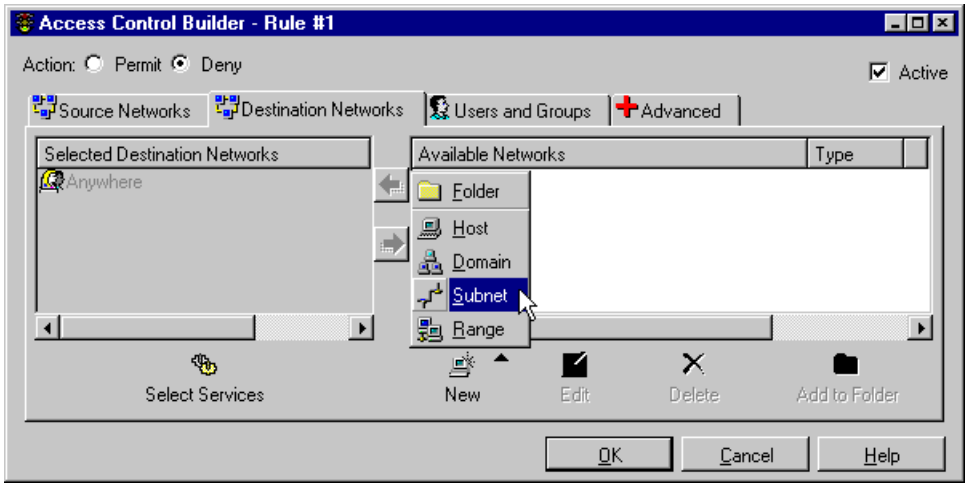
On an extranet, message traffic starts from a source and travels to a destination, either on the same network, or another network, by way of address protocols. Any host machine on any network has a unique address and can send and receive message traffic, hence it can be both a source and a destination. However, when you need to control message traffic, you must identify destination networks to direct message traffic. For example, your company (ABC, Inc.) has a relationship with a development team at an XYZ, Inc. office, and all members of that team need to communicate with all members of the product development team from your company. You can configure your network with authentication to match theirs. Once you add the XYZ network as a destination network,

Petitioner Apple Inc. - Ex. 1011, p. 24

you can then refine the access rights of anyone going to that network, e.g., limiting access to a destination network during certain times of the day. In doing so, you create an access control rule with the Destination Network information as an integral part of that rule.

AVAILABLE NETWORKS

You can create and edit network objects only in the Available Networks pane.To access the Destination Networks tab, at the Policy Console select a cell under the Destination Networks column and double-click, or click **New...** or **Edit...**. Any of these actions will open the Access Control Builder at the Destination Networks tab.



The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. You must move the network object to the Selected Destination Networks pane to make it a part of an access control rule. The checkbox located above the right pane indicates whether the access control rule for the selected network is active or disabled.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

SELECTED DESTINATION NETWORKS

In order to add a destination network object to an access control, filter, or proxy servers rule, you must move network objects from the right pane into

Petitioner Apple Inc. - Ex. 1011, p. 25

the left pane. The network objects then become Selected Destination Networks.

NOTE: *A check mark appears in the Available pane directly to the right of objects and/or folders to indicate they are active in the Selected pane.*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Destination networks pane, the Select Services and New tools remain functional, but the Edit, Delete and Add to Folder tools become unusable.

CREATING A NEW... (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

- To add a network object to an Available Networks pane, either right-click anywhere in the Policy Console window and select **New...** from the shortcut menu,
  -OR-
- click **New...**at the Policy Console, then click **New...** in the Access Control Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**.

You may also enter Optional Information.

NOTE: ***I****f you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders are a convenience that allow you to group similar network objects under a common name. You can create folders (which function like aliases) to appear in the Available Networks pane, into or out of which you can move selected networks (only while that folder is in the Available Networks pane). To make that folder an active destination network, move it from the Available Networks pane to the Selected Destination Networks pane, using the arrows, or you can double-click the network object (folder) to move it back and forth, from one pane to another.

ADDING OBJECTS TO A FOLDER

- To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Access Control Builder and select Add to from the shortcut menu
  -OR-

Petitioner Apple Inc. - Ex. 1011, p. 26

- Select the objects and click the Add to Folder tool. This will open the Add to Folder dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the SHIFT key down as you click the first and last objects of a continuous list, or by holding the CONTROL key to select individual, non-continuous objects.*

EDITING A NETWORK/OBJECT

Either right-click a cell under the Destination Networks column on the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. The Access Control Builder will appear. Select from the Available Networks pane the network object you want to edit. Then click the Edit tool on the Access Control Builder. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to that Destination Network is global.

DELETING A DESTINATION NETWORK/OBJECT

To delete a destination network object from an access control rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the rules that will be disabled due to security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

ADDING AND/OR EDITING SERVICES (PORTS)

- You can only add or edit network services (ports) to network objects in the Selected Destination Networks pane. Right-click an object in that pane and select Edit Services from the shortcut menu
  -OR-
- Select the object in that pane and click Select Services. Either action will open the Selected Services dialog box where you can add or edit network services (ports) to your selected network object.

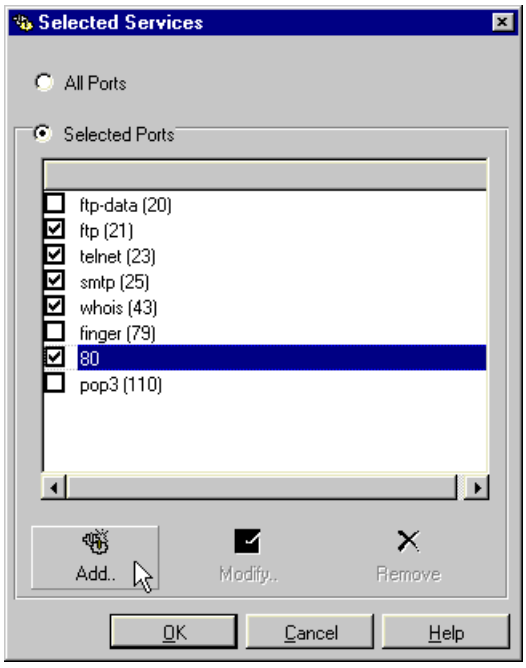
SERVICES (PORTS)

The port number is an identifier for the type of service that runs on that network; e.g. e-mailers send and receive on port 25 (the SMTP port), Web servers send and receive on port 80 (the HTTP port), and telnet is on port 23. On the Aventail ExtraNet Server, you can assign any number to any service on a network. However, the industry standard is for servers to use the commonly accepted port numbers (up to 1024) for specific services.

SELECTED PORTS

By allowing only selected services you will restrict the services that the clients can access on the destination machine.

Petitioner Apple Inc. - Ex. 1011, p. 27



DEFAULT CONFIGURATION

Prior to configuring your ports, the Aventail ExtraNet Server's default will be to allow any (all) ports for an access control rule. The Selected Services dialog box will present eight commonly used services/ports when you initially open it. You may add or delete ports via the Add/Modify Ports dialog box to build a suite of your most commonly used ports.

ADDING A SERVICE (PORT)

To add a service (port) to a rule:

1. In the Policy Console, double-click the Access Control rule that contains the network to which you want to add a port, then click Select Services at the bottom of the Selected pane,
   -OR-
   Click Add
2. Select the source or destination network to which you want to add a port. Make certain the network is in the Selected pane.
3. Click the Edit Ports tool.
4. Choose either the All Ports or Selected Ports option on the Select Ports dialog box. If you choose Selected Ports check the port number you want to assign to the network,
   -OR-
   If you choose Selected Ports, click the Add tool at the bottom of the Select Ports dialog box, and the Add Port dialog box will appear. You have the option of selecting a port name (service) from the Port: list box, or entering a from-to port range.
5. After entering your information, click **OK** on all open dialogs until you return to the Policy Console.

Petitioner Apple Inc. - Ex. 1011, p. 28

EDITING A PORT

1. To modify a port, follow steps 1 and 2 from above.
2. Select **Edit...**. The Edit Ports dialog box appears.
   The selected port number or port range appears in the appropriate boxes.
3. After entering your new information, click **OK** on all open dialog boxes until you return to the Policy Console.

DELETING A PORT

To delete a port from your suite of commonly used ports:

1. Select that port in the Select Ports dialog box, and click Delete (at the bottom of the Select Ports dialog box).
2. Click **OK** on the successive windows until you are at the Policy Console.

To simply remove the port from its access control rule without removing the port:

1. Clear the check box in the Select Ports dialog box.
2. Click **OK** on the successive windows until you are at the Policy Console.

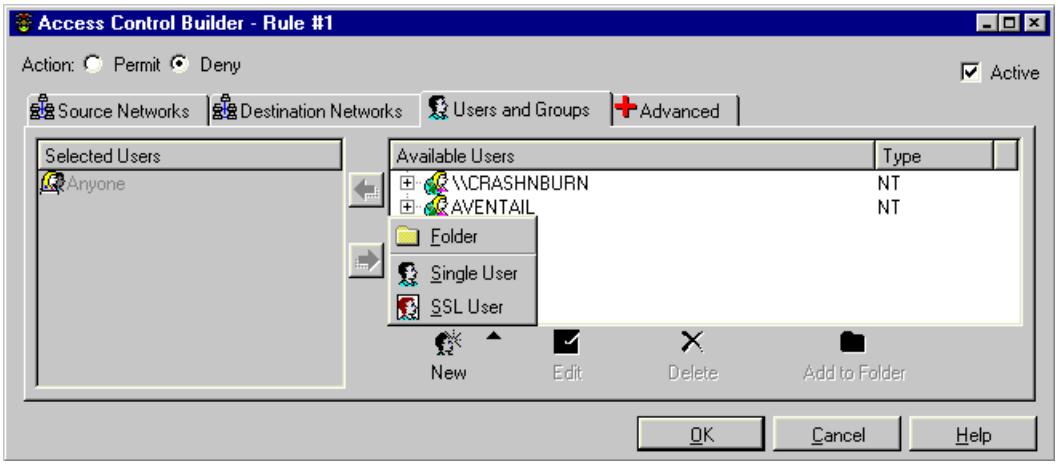
WHAT SERVICES ARE ON WHICH PORTS

When the Aventail ExtraNet Server detects the type of service carrying a client request, the service name will appear in the Select Ports dialog box.

NOTE: *The Port: list box in the Add/Modify dialog box will list the suite of ports available on your machine.*

Users and Groups

The Aventail ExtraNet Server will automatically populate the Policy Console with available (browseable) NT and NDS users and groups, as well as UNIX populations, depending on your network setups. You can add non-browseable users and edit these users. You cannot manually add groups.



You can add new single users, new SSL users, and folders. You can create these entities only in the Available Users pane of the Users and Groups tab. To add these entities to an access control rule, you must move them to the Selected pane.

Petitioner Apple Inc. - Ex. 1011, p. 29

ADDING USERS OR GROUPS

To add a single or SSL user, from the Access Control tab, either:

1. At the Policy console, select a cell in the Users and Groups column and double-click to open the Access Control Builder
   -OR-
   Click **Add...**.
   The Users and Groups tab will appear as the active tab. The Available Users pane displays your NT, NDS and UNIX (depending on your platforms) users and groups.
2. Select New | SSL, Single User, or Folder.

EDITING USERS OR GROUPS

NOTE: *You can only edit users that you manually create.*

At the Users and Groups tab, select the entity you want to modify In the Available Users pane, and either

- Right-click and select **Edit...** from the shortcut menu,
  -OR-
- Click Edit.

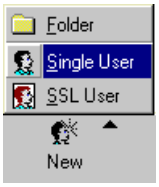
Either action will open the New User dialog box where you can enter your changes. When you finish entering your changes, click **OK**. Your changes now appear in the Available Users pane. To make those changes active in an access control rule, move the entity to the Selected pane and click **OK**.

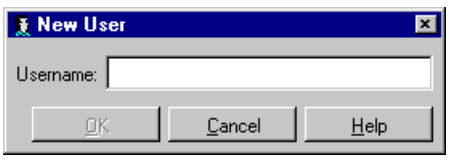
REMOVING USERS OR GROUPS

Select the entity you want to remove (delete) in the Available Users pane, and click Delete or right-click and select Delete from the shortcut menu. Depending on your User and Groups setup, a Delete Confirmation dialog box will open stating that the user or group will be deleted from the "following rules" or that specific rules will be deactivated due to security risks. Click **OK**. The Delete Confirmation dialog closes. Then click **OK** at the Access Control Builder.

SINGLE USER

The Aventail ExtraNet Server will automatically populate the Policy Console with available (browseable) NT and NDS users and groups, as well as UNIX populations, depending on your network setups. You can add single users (non-browseable; i.e., RADIUS, text file), and edit or delete them.





Petitioner Apple Inc. - Ex. 1011, p. 30

ADDING A SINGLE USER

To add a new, single user,

1. click **Add...** at the bottom of the Policy Console

-OR-

Double-click an access control rule in the Users and Groups column.The Access Control Builder will appear with the Users and Groups tab active.

2. Select New | Single User in the toolbar,

-OR-

Right-click the white space in the Available Users pane and select New | Single User from the shortcut menu. The New User dialog box appears.

3. Enter the appropriate information and click **OK**. The new user appears in the "plain" directory in the Available Users and Groups pane of the Access Control Rule.To add the new user to a rule, you must move the new user to the Selected Users pane.

DELETING A SINGLE USER

To delete a single user, make certain the single user's name shows in the Available Users and Groups pane of the Access Control Builder, select it, and click Delete in the toolbar. The Delete Confirmation dialog box will open, with the rule number and type of rule displaying in the dialog window. It warns you that either,

- the rule(s) affected by the deletion will be deactivated because of a security risk
  -OR-
- it will notify you of all the rules affected by deleting the single user.

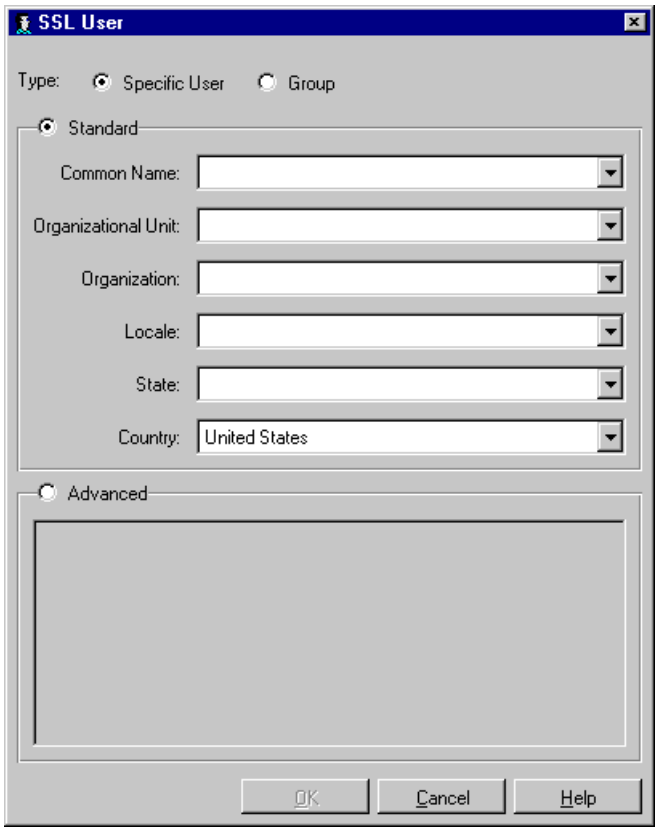
Click **OK**. If the deletion will cause a security risk, the check mark at the beginning of that rule on the Policy Console/Access Control tab will disappear, as will the check mark in the upper right-hand corner of the Access Control Builder. The ACL rule will be unavailable to the server until you reactivate it. Whether or not the deletion causes a security warning, that single user will no longer appear in the Available Users pane.

SSL USER

You can organize and maintain certificate information (RFC 1485) for users and groups via the SSL User dialog. How you organize that information depends on your certificate format, information, and the number of users requiring certificates. Once you enter certificate information into the SSL User dialog box, you can add the SSL user to Available users and groups

To organize standard or advanced SSL certificate information by specific users or by groups, click New at the Users and Groups tab and select SSL User, or right-click in the Available pane at the users and Groups tab and select New | SSL User from the shortcut menu.

Petitioner Apple Inc. - Ex. 1011, p. 31



You can enter distinguished name information through either the Standard or Advanced sections of the SSL User dialogs.

ENTERING STANDARD CERTIFICATE INFORMATION

You must type appropriate certificate information into each text box. The text boxes will populate as you add information for successive SSL users. This will allow you to use the "pull-down" features of the text boxes.

ENTERING ADVANCED CERTIFICATE INFORMATION

You can cut distinguished name information from a certificate via a text viewer, and paste it into the Advanced window of the SSL User dialog.

ENTERING OPTIONAL INFORMATION

If you enter an optional name, it will appear in the Available pane on the Users and Groups tab after you click **OK** to close the SSL User dialog box. Otherwise, the distinguished name will appear in the SSL User tree.

Advanced

You can access the Advanced tab via the Access Control Builder and Filter Builder. On the Advanced tab, you can:

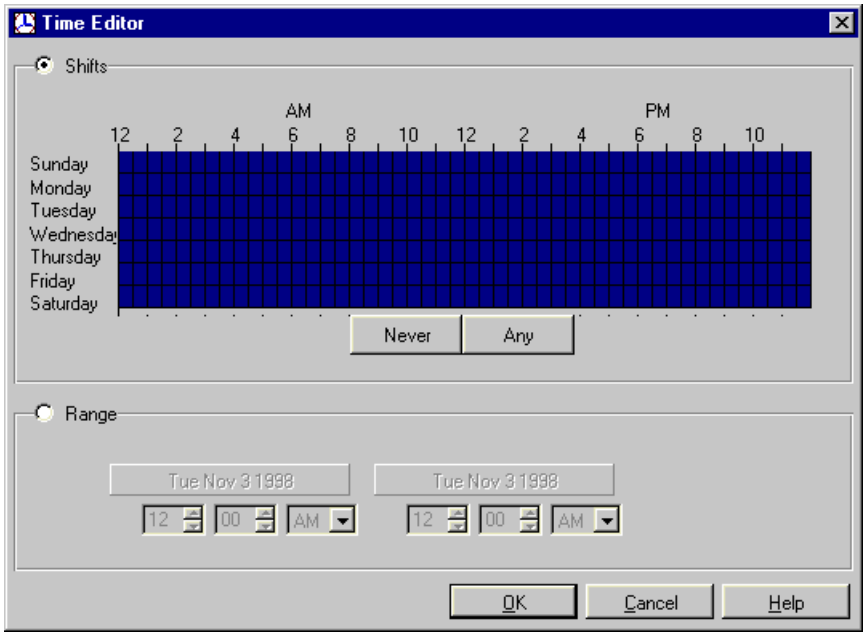
- add time-based restrictions to access rules,
- match authentication between client and server,
- establish a required key length for client access,

Petitioner Apple Inc. - Ex. 1011, p. 32

- and configure the network commands for the Aventail ExtraNet Server.

TIME ATTRIBUTES

In addition to controlling access by destinations, users and groups, and authentication, you can also control access by days of the week and hours of the day. This means you can limit people to coming in only during business hours, or, limit a contractor to coming for only a two-week period.



TIME EDITOR

You modify the default time-based rule of "Any" via the Time Editor. To do that, select the Access Control Rule | Advanced tab. You will see the default configuration Any in the Time pane of the Advanced tab. To change that configuration, select Edit on the Advanced tab and the Time Editor appears. The Time Editor will display the Shifts (24-hour/7-day) grid as completely blue.

Petitioner Apple Inc. - Ex. 1011, p. 33

- To completely limit access by time-based rules, click Never. The 24-hour/7-day grid clears to grey.
  -OR-
- Select (either or both?) the Shift or Range options on the Time Editor to configure a limited, time-based rule.

CONFIGURING SHIFTS

1. Click on any number of squares in the 24/7 grid to designate access hours and day(s),
   -OR-
   Click and drag your cursor to include start/end access times from a specific start day to end day of the week.
2. Click **OK** on the Time Editor and the access days/hours appear in the Time window of the Advanced tab.
3. Click **OK** and the days/hours appear on the Policy Console in the Times cell of the rule to which you applied time-access constraints.

Range

1.Upon selecting the Range option on the Time Editor, the 24/7 grid clears to grey.

2. Click the starting date button (left side) and a calendar dialog box opens.
3. Select your starting date and time.
4. The calendar closes and the starting date appears on the starting date button.
5. Repeat the process with the ending date button (right side) and calendar.
6. Click **OK** on the Time Editor and the start/end dates/times appear in the Time window of the Advanced tab.
7. Click **OK** and the start/end dates appear in the Times cell of the rule to which you applied time-access constraints.

ADDING AUTHENTICATION MATCHING

Authentication matching simply means that you configure an access control rule to offer a specific or several authentication methods to match an incoming or outgoing access request. In order to match authentication requirements between client and server, you must first load and assign the authentication method(s) to a source network. You can load the authentication modules via the Add/Edit button of the Authentication Methods tab on the Authentication Builder. Once you configure and load the modules, they appear in the windows of the Authentication Methods tab and the Authentication Matching window on the Advanced tab. However, they are not enabled.

- Click Select All to enable all the loaded modules,
  -OR-
- Check specific modules to enable them.
- Click **OK**.

ADDING KEY LENGTH REQUIREMENTS

This is a new feature in the ExtraNet Center. The key length requirement can force 128-bit encryption to certain resources when a client allows a combination of null, 56-bit and 128-bit encryption. You do this via the

Petitioner Apple Inc. - Ex. 1011, p. 34

Advanced tab. If you allow 40-, 56-, and 128-bit encryption, the server will always try to establish a 128-bit session, but if the client is restricted to 40-bit strength due to export restrictions, the server will "dumb down" to the 40-bit session. You can restrict access to sensitive information to 128-bit uses with

Adding network commands

To enable basic network commands (Traceroute, Ping, UDP, Bind, and Connect) select the Any Commands option on the Advanced tab. To enable specific commands, select the Specific Commands option which will make the commands available, then check the desired commands in the Authentication Matching window.

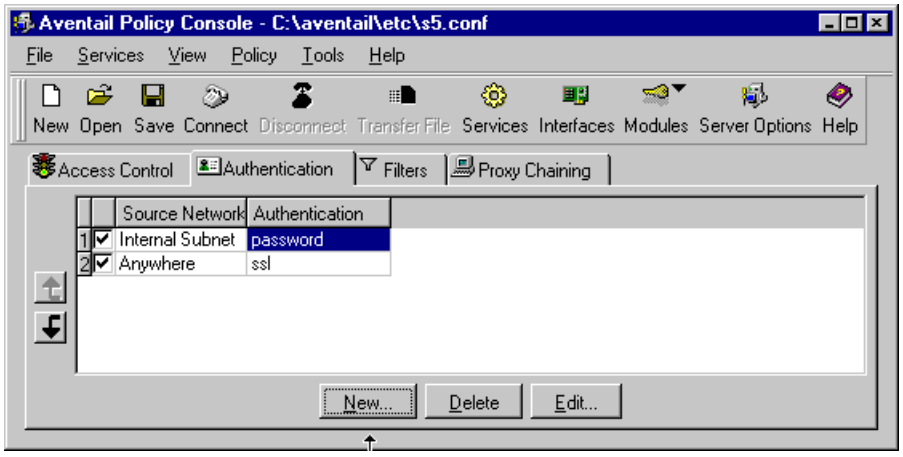
Petitioner Apple Inc. - Ex. 1011, p. 35

Authentication

When the server receives an incoming client request, it will poll its suite of authentication rules in descending order to match the user's source (IP, host name, domain name, range, or subnet) to a source in an authentication rule. When the server finds a match, it then compares authentication methods available to the client source against methods the client offers the server. The server then selects the appropriate method for the client if it is in the Config file.

- If the source of the client request is "Anywhere," the server will match this rule and look no further.
- If the server cannot match a client source, it will deny the connection.
- If the client cannot use any source the server specifies in an authentication rule, the server will deny the connection.

NOTE: *The Aventail ExtraNet Server will not start without authentication rules.*



Each authentication rule consists of two configurable elements:

- the source networks,
- and the authentication method(s) assigned to those networks.

As an example (see above), rule #1 requires a user coming from the company's internal subnet to authenticate with a username and password. Rule #2 requires the user to subauthenticate with username/password; i.e., if the client comes from anywhere other than the internal subnet, it must first establish an SSL (encrypted) session, then authenticate with, in this case, username/password as a secondary method. You must first select a source network before you can apply an authentication method to it.

Changing rule order

- To establish the order of a rule, select the entire rule or a cell of that rule. Use the up/down arrows located on the left side of the Authentication tab to move the rule to its new position in rule order.
  -OR-

Right-click a selected cell of the rule you want to reorder, and select the "move up" or "move down" arrow commands from the shortcut menu.

Adding authentication rules

- On the Authentication tab, click New...
  -OR-
- Right-click anywhere in the white area of the Authentication tab and select New... from the shortcut menu.
  -OR-
- Double-click anywhere in the white area of the Authentication tab.Any of these actions will open the Authentication Builder.

Editing authentication rules

- At the Authentication tab, select the cell in a rule that you want to modify, and click Edit...
  -OR-
- Select the cell in a rule that you want to modify, right-click and select Edit... from the shortcut menu.
  -OR-
- Double-click any cell of a rule.
  -OR-
- Use the arrow keys to move the highlighted focus to a desired cell, then click **Enter.**
- Any of these actions will open the Authentication Builder at the appropriate tab for the selected cell, with the rule number of the selected cell displayed in the title bar.

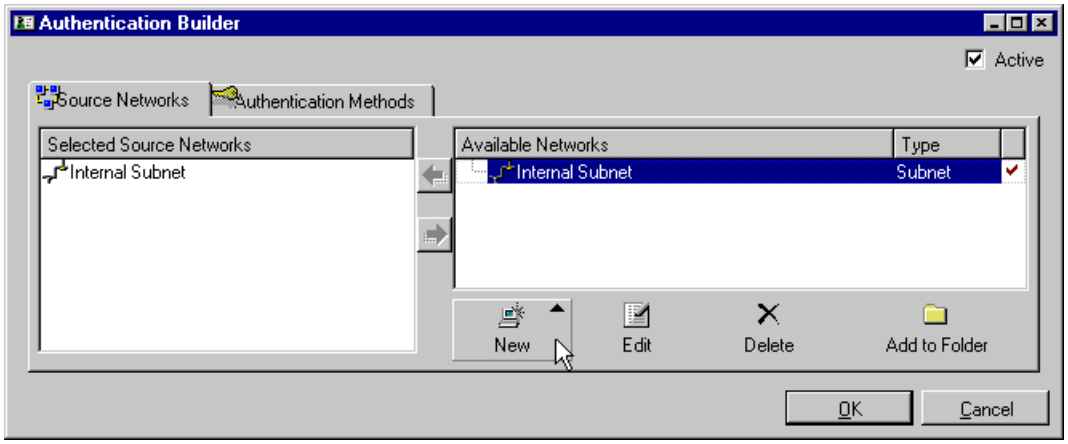
Deleting authentication rules

- At the Authentication tab, select the entire rule or any cell in that rule. Click **Delete**.
  -OR-
  Right-click the selected rule or cell, and select Delete from the shortcut menu.
  -OR-
  Use the arrow keys to move the highlighted focus to a desired cell, then click **Delete**.

Petitioner Apple Inc. - Ex. 1011, p. 37

AUTHENTICATION BUILDER

You can configure and view authentication rules via the Authentication Builder. The configurable properties of the Source Networks tab plus the contents of the Authentication Methods tab constitute an authentication rule.



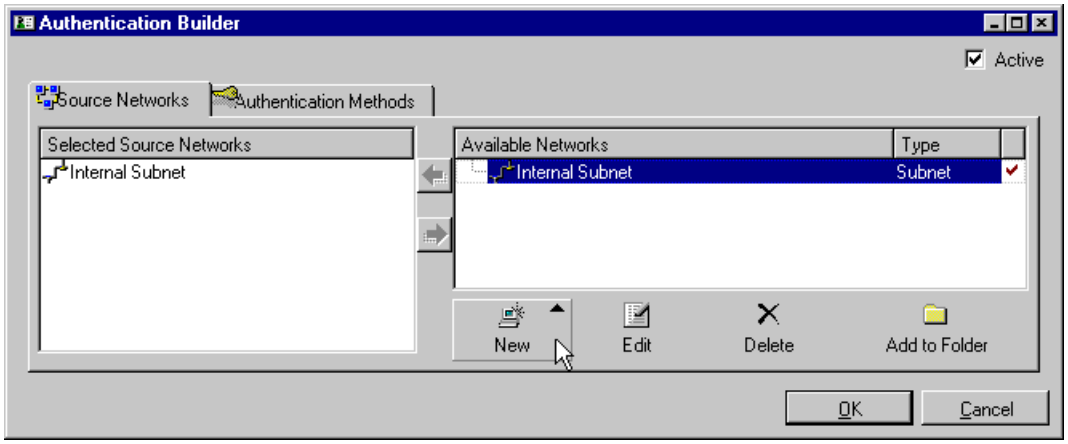
"Active" checkbox in the upper right-hand corner of the Authentication Builder will temporarily deactivate rules without having to delete them.

Via the Source Networks tab you can configure the network information for your authentication rule.

Via the Authentication Methods tab of the Authentication Builder, you can configure, load and enable the authentication method for your authentication rules.

Source Networks

The Aventail ExtraNet Server uses two, integral, configurable elements to create authentication rules. The source network is one part, and authentication method is the other.



Petitioner Apple Inc. - Ex. 1011, p. 38

AVAILABLE NETWORKS

The right pane (Available Networks) is for adding network objects. You can create and edit network objects only in the Available pane. In order to assign an authentication method to the source network, you must move the network object to the Selected Source Networks pane.

You can create five types of network objects and assign them unique names:

- Folders
- Hosts
- Domains
- Subnets
- Ranges

SELECTED SOURCE NETWORKS

In order to add a source network object to an authentication rule, you must move network objects from the right pane into the left pane. The network objects then become Selected Source Networks.

NOTE: *A check mark appears in the Available pane to the right of objects and/or folders to indicate they are active in the Selected pane. (See above).*

TOOLS

The tools located at the bottom of the Access Control builder become active as you roll your mouse over them: All of the tools are functional only when you select a network object in the Available Networks pane, or create a new network object (host, domain, subnet or range). When you select a network object in the Selected Source Networks pane, the **New** tools remain functional, but the **Edit**, **Delete** and **Add to Folder** tools become unusable.

CREATING A NETWORK/OBJECT... (FOLDER, HOST, DOMAIN, SUBNET, RANGE)

To add a network object to an Available Networks pane, either right-click anywhere in the Available pane and select New... from the shortcut menu,
-OR-
click **New...** at the Source Networks tab of the Authentication Builder and select the type of network object you want to add. A Network Objects dialog box will appear with the object type (folder, host, domain, subnet or range) in the title bar. Enter the name or address for the object and click **OK**.You may also enter Optional Information.

NOTE: *If you enter any name or address in an Optional Information text box, that name/address will appear in the Available Networks pane. If you delete the optional name/address, the object's name defaults to the name/address in the text box above the Optional Information text box.*

FOLDERS

Folders are a convenience that allow you to group similar network objects under a common name. You can create folders (which function like aliases) that will appear

Petitioner Apple Inc. - Ex. 1011, p. 39

in the Available Networks pane, into or out of which you can move selected networks and groups (only while that folder is in the Available Networks pane). To make that folder an active source network, move it from the Available Networks pane to the Selected Source networks pane, using the arrows, or you can also double-click the network object (folder) to move it back and forth, from one pane to another.

Adding objects to a folder

To add network objects to a folder, right-click on those objects while they are in the Available Networks pane of the Source Networks tab and select **Add to** from the shortcut menu
-OR-
Select the objects and click the **Add to Folder** tool. This will open the Add to Folder dialog box.

NOTE: *If you have more than one network object to add to a folder, multi-select the objects by either holding the SHIFT key down as you click the first and last objects of a continuous list, or by holding the CONTROL key to select individual, non-continuous objects.*

Editing an authentication source network/object

Right-click a cell under the Source Network column on the Authentication tab of the Policy Console and select **Edit...** from the shortcut menu, or double-click the cell. Either action will open the Authentication Builder at the Source Networks tab. Select from the Available pane the network object you want to edit.

Then click the **Edit** tool. The Network Objects dialog box appears. You can enter new or edit existing information. Click **OK** after entering or editing your information. The change to that Source Network is global.

Deleting a source network/object

To delete a source network object from an authentication rule, select the object in the Available Networks pane and click the Delete tool. A Delete Confirmation dialog box will appear displaying the network object you selected for deletion, and the access control rules that will be disabled due to the security risks as a result of the deletion. Clicking **OK** will complete the deletion of the network object.

Authentication Methods

The Authentication Methods tab is where you select an acceptable authentication method for a source network. This tab displays all loaded authentication modules. To apply an authentication method to a source network, check the box of the desired method. You can also add (load) or edit authentication modules via the Authentication Methods tab.

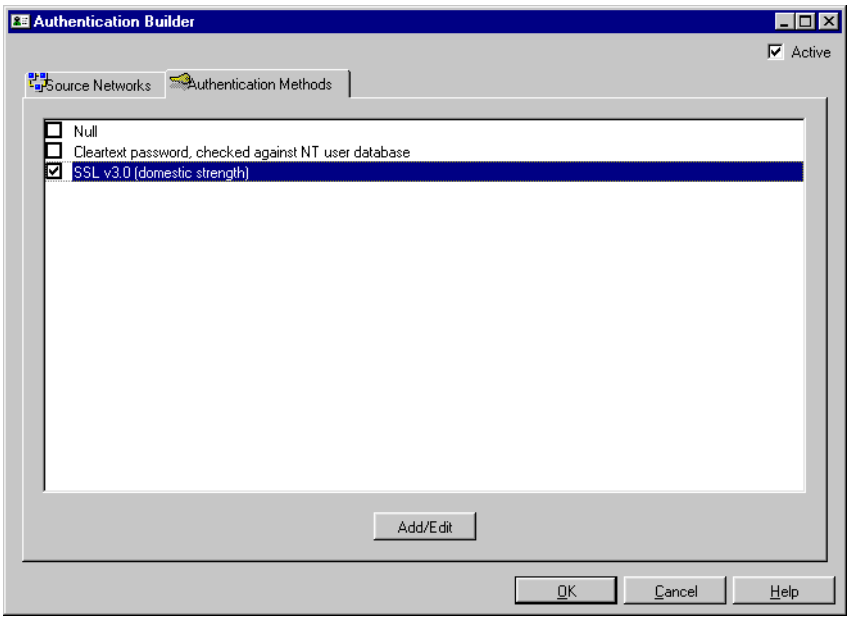
If you select more than one method and the client can authenticate with any of them, the server will select the first authentication rule (#1 of the ordered list of authentication rules). You can configuring the Aventail ExtraNet Server to offer multiple authentication methods.

You can also configure the server to require encrypted messages, or SSL, without requiring authentication, or to require only authentication without encryption. Customarily,

Petitioner Apple Inc. - Ex. 1011, p. 40

you will require subauthentication when using SSL, which means that you specify an authentication method within the SSL module.

NOTE: *Loading and checking both SSL and an additional authentication method at the Authentication Methods tab DOES NOT mean that the authentication will automatically encrypted. You MUST identify the authentication you want to encrypt (called "subauthentication" via the SSL module if you want to assure that the server will encrypt your authentication*



ADDING OR EDITING AUTHENTICATION MODULES

To load, configure and edit an authentication module, click **Add/Edit** (at the Authentication Methods tab of the Authentication Builder) to open the Authentication Modules dialog box. Once you have loaded and configured your authentication modules, and they appear at the Authentication Methods tab, you can.

NOTE: *You must first select a source network before you can apply an authentication method to it.*

- Click Select All to make all loaded authentication available for the source network
  -OR-
- Check only specific method(s) for the selected source network.
- Click **OK** to close the Authentication Builder. This puts you back at the Policy Console. You will see the new rule on the Authentication tab.

SUBAUTHENTICATING (WITH SSL)

If you select only CHAP, CRAM or password for an authentication method, clients will authenticate but the traffic that matches the specific rule will be in the clear; i.e., not encrypted. If you select SSL (encryption) and you do not specify a secondary

Petitioner Apple Inc. - Ex. 1011, p. 41

authentication method within the SSL module, the server will encrypt that traffic but not require authentication.

CONFIGURE SSL

To both encrypt and authenticate traffic, you must correctly configure SSL:

1.First, load the desired authentication methods (CHAP, CRAM, or password).
2.Begin the process of loading SSL, and at the Authentication Modules dialog box select the Client Auth. tab of the SSL module.

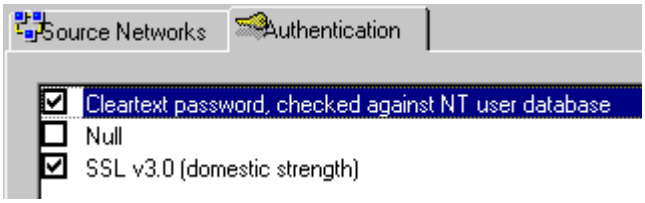
3.Enable "Require Client Authentication," and the Secondary Authentication window will become active and display the loaded secondary authentication methods.

4.Select the desired secondary authentication method, and click OK. Return to the Authentication Methods tab of the Authentication Builder. You will see the secondary methods and SSL as available authentication methods.

If you select SSL as the only method for your authentication rule, the server will encrypt (transparently) and require authentication based on the secondary authentication method.

This means that clients only have the option of SSL (encryption) and must subauthenticate with the NT username and password (when coming from a specified source).

If you select SSL and a secondary method, you are efffectively giving the server a choice of methods.



This means the clients have the option of using SSL (encryption) and must subauthenticate with NT username and password,

-OR-

Clients can use the NT username and password without encryption (when coming from a specified source).

Petitioner Apple Inc. - Ex. 1011, p. 42

Authentication Modules

The Aventail ExtraNet Server used authentication rules to check incoming (server) and outgoing (client) requests for access. An authentication module is one of two integral, configurable elements of any authentication rule. The source network is the other.

LOADING A MODULE

Select a CHAP, CRAM, cleartext password, or SSL module from the Add Module dialog box, then click **OK**. This loads the module into, and opens, the Authentication Modules dialog box for configuration. The configurable properties of each module are explained below:

CHAP, CHECKED AGAINST A RADIUS SERVER

Incoming module that uses the CHAP protocol for transmission.

Password checking is against a RADIUS user database.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CHAP, CHECKED AGAINST A PLAIN TEXT FILE

Incoming module that uses the CHAP protocol with MD5. Password checking is against a specified password file.

- Password File: Verification is against this password file. The file must contain one username/password combination, separated by whitespace, per line.

CRAM, CHECKED AGAINST A RADIUS SERVER

Incoming module that uses the Challenge-Response Authentication Method against a RADIUS database.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.
- Always prompt for password without consulting RADIUS server:

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.

Petitioner Apple Inc. - Ex. 1011, p. 43

- Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CRAM, CHECKED AGAINST AN ACE SERVER

Incoming module that uses the Challenge-Response Authentication Method via SecurID tokens against a user/token database on an ACE server. Requires no configuration.

CLEARTEXT PASSWORD, CHECKED AGAINST NT USER DATABASE

Incoming module that applies cleartext-password checking against the Windows NT user database. The server authenticates against LognUser value, for both member and trusted domains.

WARNING: *You must disable the NT Guest Account on the NT server. If you do not, the NT logon module will authenticate any user.*

AUTHORIZATION SCOPE

- SOCKS Server Only: Default value. Verifies password with only the local user database on the server.
- SOCKS Server and Windows NT domains: Verifies the password with the local user database on the server as well as on any trusted domains. If you check Let User Specify Domain, the users can specify which domain to use for authentication. This is an appropriate option when users have accounts on several domains, but different access rights. The format for a user-specified domain is domain\\username.
- Allow user password update: Prompts user to update their password (check on this).
- Export additional user information: Forwards authentication information to another server. It eliminates having to enter authentication information at every server.

CLEARTEXT PASSWORD, CHECKED AGAINST NETWARE

Incoming module applied to NetWare servers using either NDS (NetWare Directory Services) or Bindery NetWare function calls. Because this module needs to make NetWare C Interface Library function calls, the NetWare client for Windows NT must be installed on the same server as the Aventail ExtraNet Server.

NDS (NetWare Directory Services) Authorization: If you check this, the ExtraNet Server will perform authentication against the local

- Novell NDS server on the network. The Aventail ExtraNet Server will always attempt Novell NDS before any specific bindery servers listed in the NetWare Bindery section.
    - Name-Enter user name (and context); e.g., kevin.xena.fox.
    - Password-Enter required password.
    - Tree-Select appropriate tree from pulldown menu.
- NetWare Bindery Servers: If checked, the Aventail ExtraNet Server will attempt authentication of clients against one or more Novell NetWare bind-

Petitioner Apple Inc. - Ex. 1011, p. 44

ery-based servers. The Aventail ExtraNet Server will attempt to authenticate users against each listed server until 1) one is found that positively authenticates the user or 2) the list of servers is exhausted. You dictate the server order in the listbox, which you can rearrange via the up and down arrows.

Export additional user information: Forwards authentication information to another server.

CLEARTEXT PASSWORD, CHECKED AGAINST A RADIUS SERVER

Incoming module that checks passwords against a RADIUS user database, caches credentials, and forwards user authentication information.

GENERAL TAB

- RADIUS server: The name of the RADIUS database server.
- RADIUS password: The RADIUS database server logon.
- Export additional user information: Forwards authentication information to another server. It eliminates having to enter authentication information at every server.
- Inherit Ascend-Data-Filter rules: Allows administrators to use Ascend RADIUS rules in conjunction with the Aventail ExtraNet Server.

CACHING TAB

- Cache Credentials: Check to enable cache file.
- Cache file: Name of RADIUS caching file.
- Lifetime (hours): Number of hours cache retains credential information.

ADVANCED TAB

- RADIUS identifier: The NAS identifier of your RADIUS request. If empty, this defaults to hostname.
- Transmission timeout: The number of seconds before the server attempts retransmissions and/or using auxiliary servers, if needed.

CLEARTEXT PASSWORD, CHECKED AGAINST A PLAIN TEXT FILE

The module applies password checking against a specified password file.

Filename: Verification is against this password file. The file must contain one username/password combination, separated by whitespace, per line.

Export additional user information: Forwards authentication information to another server.

SSL v3.0

Incoming module that applies one or more encryption algorithms to message traffic, plus compression.

GENERAL TAB

- Acceptable Ciphers: RC4, DES, NULL (no encryption), Diffie-Hellman (not recommended except for testing).
  Advanced... button: See below.

Petitioner Apple Inc. - Ex. 1011, p. 45

- Credentials Cache
  SSL session resumption requires that you store certificate information. This box allows to specify where the file will be stored via the browse button.
  Cache file: Specifies the storage file for certificate information. If you do not specify a file, the default is sslsrvdata in the temp directory.
  Lifetime (hours): Specifies how long to keep data before considering it stale.
- Miscellaneous
  Max. Certificate Chain Length: You specify the maximum length for a certificate chain, starting with not less
  than two certificates.
  Enable Compression: Transparently compresses encrypted data, depending on available network bandwidth.

ADVANCED BUTTON

The Advanced SSL Server Option Dialog box allows combinations of encryption strengths plus various encryption standards. Its default configuration allows 40- to 128-bit encryption modes.

- Advanced RC4 Options
  RC4 with MD5 (default cipher suite, combining excellent security with speed).
  RC4 with SHA (a more secure suite, but considerably slower).
  RC4 exportable (40-bit) with MD5 Legal encryption strength for U.S. export (clearing checkbox disables 40-bit encryption).
- Advanced DES Options
  DES with SHA (very secure but slow cipher suite).
  Triple DES with SHA (more secure suite than above, but even slower).
  DES exportable (40-bit) with SHA (legal encryption strength for U.S. export) (clearing checkbox disables 40-bit encryption).
  NULL with SHA-Offers stronger protection to authenticated (not encrypted) traffic.
  NULL with MD5-Offers faster protection to authenticated (not encrypted) traffic.
  Reset Defaults Restores all Advanced RC4 and DES option to fully enabled state.

CERTIFICATES TAB

- Certificate File Specifies the filename which contains the certificate information created by the Certificate Wizard. Note that this is optional. It is only needed if client-side authentication is required.
- Certificate information: Displays information about the specified certificate file.
  Password-Password for certificate file.
  Reset- Clears the Certificate File and Certificate Information fields.

CERTIFICATE AUTHORITIES TAB

- Roots File - Specifies a filename containing the root(s) CAs that the client trusts. If no file is specified, any/all roots are allowed.
  Add: Reads a file containing trusted roots and adds its contents to the roots

Petitioner Apple Inc. - Ex. 1011, p. 46

file.
Remove - Deletes the highlighted trusted root from the roots file.
Describe - Pops up a box displaying more information about the highlighted root.
Reset - Clears the Roots File field.

CLIENT AUTHENTICATION TAB

- Require Client Authentication: Enables client authentication.
- Cache File - Specifies the file in which the user information associated with client authentication will be stored. If you do not specify a file, the default is *sslsrvdata* in the temp directory.
- Client certificates are:- “Never asked for” (a secondary authentication method must be used since the client certificates will not be used), optional (secondary authentication may be used in addition to the optional client certificates), “required” (secondary authentication may be used in addition to the required client certificates).
- Secondary Authentication Methods:- NULL (default), SSL (specifies the client authenticate itself with its own certificate as part of the SSL handshake). Other methods, like password, CRAM and CHAP specify that specific method as the secondary method, over the SSL-encrypted channel.

If you select both SSL and other methods (other methods only appear if you load them prior to subauthenticating), the server will attempt SSL first, and attempt to authenticate with other methods only when SSL authentication fails.

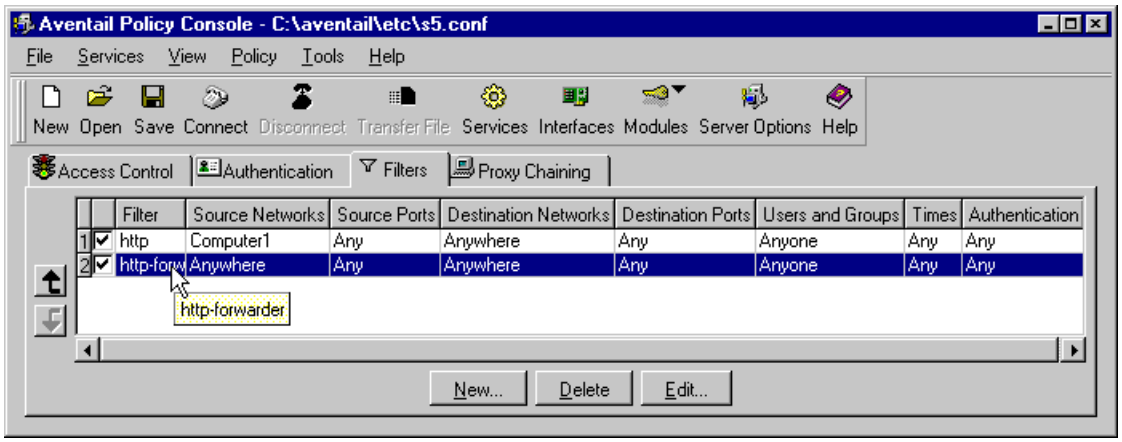
Petitioner Apple Inc. - Ex. 1011, p. 47

Filtering

HTTP content filtering can be an integral part of your access control rules for any network in your system. With the Filter Builder you can use HTTP filtering to control URL content for Source/Destination Network, and Group/User access. For example, you can apply HTTP filtering with time-based parameters, to a group (Marketing).

Marketing will not have HTTP access to:

- URLs of dating and introduction services, extreme/gross/indecent content, gambling or gambling
- information, sex content, or UseNet news sites,
- from 8 a.m. to 6 p.m., Monday through Friday.



CAUTION: *You cannot apply two filters to the same rule. The server will apply the first filter it finds for a rule and look no further.*

HTTP Content Filter

The HTTP Content filter offers both fine-grained, text-editable content control (Aventailfilter), as well as a predefined definition file (SmartFilter) of "deny" categories. Usually, you will use the text-editable filter only when content gets past the SmartFilter and continues to the end user.

HTTP Authentication Forwarding filter

The HTTP Authentication Forwarding filter allows you to forward user credentials in the HTTP header to an IIS Web server or any Web server that supports the same protocol(s) used by the Aventail ExtraNet server. This eliminates the need to repeatedly enter authentication information.

NOTE: *The forwarding filter does not require configuration.*

Petitioner Apple Inc. - Ex. 1011, p. 48

Adding Filtering Rules

At the filters tab of the Policy Console,

- Double-click in the white space of the Filters tab,
  -OR_
- Right-click and select New,
  -OR-
- Click New.

Any of these actions will open the Filter Builder. It is with the Filter Builder that you configure and enable a filter.

Editing Filtering Rules

At the Filters tab, select the appropriate cell of the rule you want to edit:

1. Right-click and select **Edit...** from the shortcut menu,
   -OR-
2. Click **Edit...**Either of these actions will open the Filter Builder where you can make your changes.

Removing Filtering Rules

At the Filters tab, select the whole rule or a cell of the rule you want to delete.

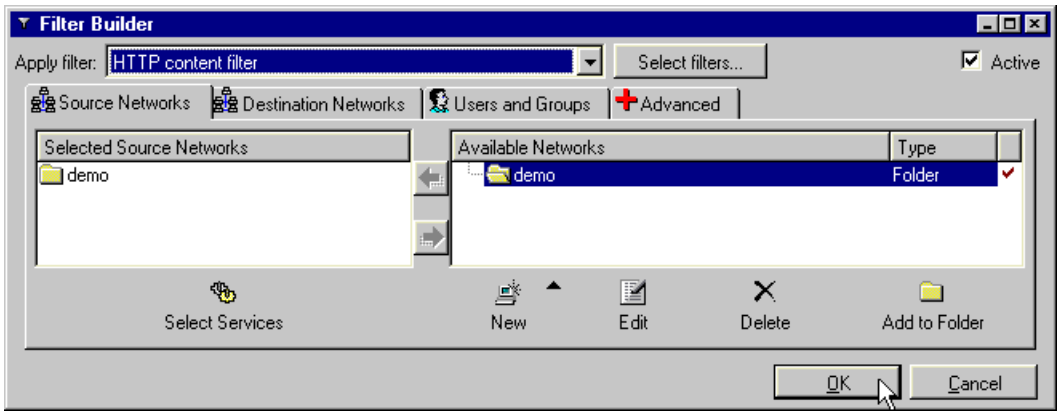
1. Right-click and select **Delete** from the shortcut menu,
   -OR-
2. Click **Delete**.Either action will remove the rule.

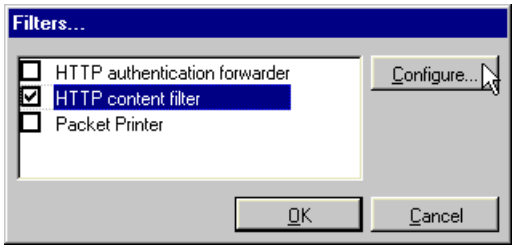
FILTER BUILDER

With the filter builder you can apply HTTP content filtering, HTTP authentication forwarding, and packet printer filtering to

- Source Networks
- Destination Networks
- Users and Groups
- and content available through the Advanced tab of the Filter Builder.

Petitioner Apple Inc. - Ex. 1011, p. 49





ADDING FILTERING TO A NETWORK, USER/GROUP, OR TIME-BASED RULE

1. At the Filter Builder, select the appropriate tab and network or user/group object to which you will apply filtering.

NOTE: *Make certain that the object appears in the "Selected" pane.*

2. Once you select your object, click Select Filters.... This opens the Filters... dialog box.
3. Enable the appropriate filter and click **OK**.The enabled filter now appears in the Apply Filter... text box of the Filter Builder.

NOTE: *Checking the HTTP Content filter activates the Configure... button.*

The new filter rule appears on the Filters tab.

EDITING FILTERING FOR A NETWORK, USER/GROUP, OR TIME-BASED RULE

At the Filter tab, select the whole rule or a cell of the rule you want to edit.

- Right-click and select Edit... from the shortcut menu,
  -OR-
- Click Edit...,
  -OR-
  Double-click the selected cell.
- Any of these actions will open the Filter Builder. Make the appropriate changes, and

Petitioner Apple Inc. - Ex. 1011, p. 50

- click **OK**. The changes will appear at the Filters tab.

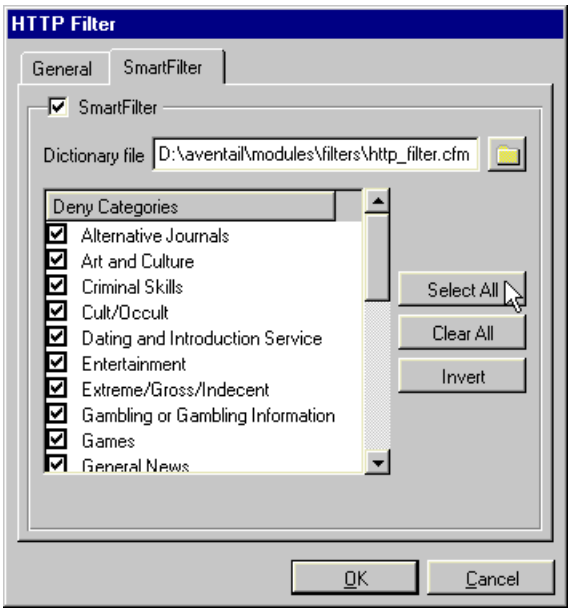
DELETING FILTERING FROM A NETWORK, USER/GROUP, OR TIME-BASED RULE

At the Filters tab, select the rule you want to delete, and

- Click Delete,
  -OR-
- Right-click and select Delete from the shortcut menu.This removes the rule from the Filters tab.

HTTP Content Filter

The HTTP filter will allow you to make sophisticated policy decisions, not just "user X can (or cannot) connect to host Y." In addition to controlling URL access, you can remove content, strip HTML tags, and deny JAVA and ActiveX controls. The HTTP filter currently consists of two filters:



- SmartFilter -- SmartFilter blocks URLs based on deny categories in a definition file supplied with the HTTP filter. You must load the dictionary file to enable the SmartFilter to block URLs.
- General tab (Aventail) -- The Aventail filter offers fine-grained, text-based control to block Netscape Plug-ins, JAVA applets, and ActiveX controls. You must load the filter configuration file to block HTTP content.

CONFIGURING AND LOADING THE HTTP CONTENT FILTER

To configure and enable the SmartFilter module, select the SmartFilter tab of the HTTP Filter dialog box.

1. Check the SmartFilter box. Browse for the dictionary file

`(aventail\modules\filters\http_filter.mod),`

2. select and load it into the text box.

Petitioner Apple Inc. - Ex. 1011, p. 51

3. At the Deny Categories window, check the categories you want to exclude,
   -OR-
   click Select All.

NOTE: *The Invert button reverses "deny" selections within the Deny Categories window. It does not clear them.*

4. Click **OK**. This returns you to the Filters dialog box.
5. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to deny access to the URLs in the selected categories. You can apply it to any network, user, group or time-based rule.

To configure and enable the Aventail filter (General tab), select the General tab of the HTTP Filter dialog box.

1. Check the Aventail box.
2. Browse for and select the filter file:

`(aventail\modules\filters\http_filter.cfm)`. text-editable file.

3. Click **OK**. This returns you to the Filters dialog box.
4. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to remove Netscape plugins, JAVA applets, ActiveX controls, etc. from HTTP content. You can apply it to any network, user, group or time-based rule.

To configure and enable the Aventail filter (General tab), select the General tab of the HTTP Filter dialog box.

1. Check the Aventail box.
2. Browse for and select the filter file

`(aventail\modules\filters\http_filter.cfm)`. text-editable file.

3. Click **OK**. This returns you to the Filters dialog box.
4. Click **OK**.

The HTTP Content filter now appears in the Apply filter: text box at the Filter Builder, ready to remove Netscape plugins, JAVA applets, ActiveX controls, etc. from HTTP content. You can apply it to any network, user, group or time-based rule.

Petitioner Apple Inc. - Ex. 1011, p. 52

Proxy Chaining

Proxy chaining is when one SOCKS server acts as a gatekeeper to route requests for information that resides behind another SOCKS server. In this capacity, the gatekeeper server evaluates its security policies to authenticate the user (client) request and determine if the user has access to the requested destination. If the user request is valid, the gatekeeper server acts as a client and proxies the user request to another SOCKS server by authenticating to the secondary SOCKS server. If the secondary server has access to the destination, the user passes through to the destination.

You can assign a destination to a server's address, so all requests to this destination will be proxied (forwarded) to that server. Additionally, you can prioritize proxy servers.

To proxy chain a server, you configure the proxy server name and address, the name of a fallback server (optional), the destination network, and the network services (ports).

Adding a Proxy

At the Proxy Servers tab on the Policy Console,

- Double-click in the white space
  -OR-
- click New...,
  -OR-
- Right-click and select New... from the shortcut menu.

Any of these actions will open the Proxy Chain Builder.

Editing a Proxy

At the Proxy Servers tab, select a cell of a rule that you want to edit, and

- right-click and select Edit... from the shortcut menu,
  -OR-
- click Edit....

Either action will open the Proxy Chain Builder at the appropriate tab.

Deleting a Proxy

At the Proxy Servers tab, select the proxy rule you want to delete, and

- Right-click and select Delete from the shortcut menu,
  -OR-
- click Delete.

Proxy Chain Builder

The Server tab allows you to identify and configure the proxy and fallback servers for the destination network. The default status of the Server tab is to allow a direct connection, not proxied.

Petitioner Apple Inc. - Ex. 1011, p. 53

To proxy a server, you will need to

- select the Proxy option on the Server tab of the Proxy Chain Builder,
- enter host and port information for the proxy server,
- and enter host and port information for the fallback server, if you use a fallback server.

Additionally, you need to select a SOCKS version.

Adding a primary/fallback host and port

Select the Proxy option on the Server tab. If you will use a fallback server, enable the Use Fallback option. Enter a qualified name, fully qualified name or IP address for the primary (and fallback) host. Enter a single port.

Editing a primary/fallback host and port

At the Proxy Servers tab on the Policy Console, select the cell containing the information you want to edit, and either right-click and select Edit,
-OR-
Click Edit. The Proxy Server Builder will open at the correct tab for your edits. When you finish entering the new information, click **OK** to return to the Policy Console.

Determining SOCKS version

Select a SOCKS version option or click Detect, then click **OK**.

Active/disabled (checkbox)

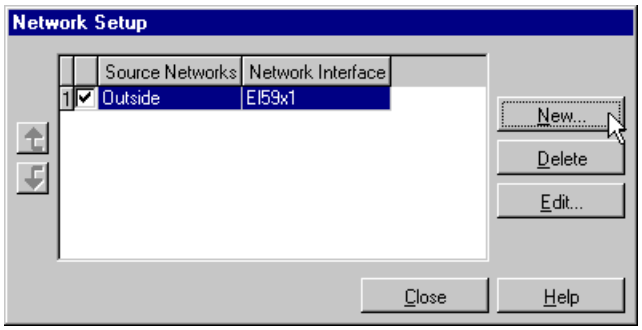
The checkbox in the right-hand corner of the Proxy Chain Builder indicates the enabled/disabled status of the proxy rule. This information corresponds to the checkmark at the beginning of each Access Control rule.

Petitioner Apple Inc. - Ex. 1011, p. 54

Network Setup

Network Setup is for "multihomed" servers (a server with two or more installed network interface cards). To properly configure your network setup you must specify what internal and external network traffic goes to which network interface cards (NIC). You do this with "routing rules."

NOTE: *To neutralize IP spoofing attacks you must properly configure multihomed servers.*

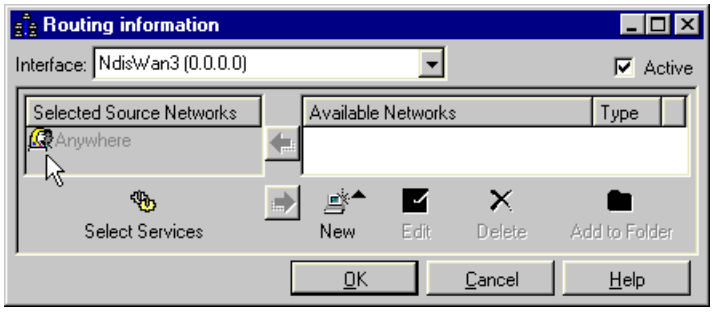


To correctly configure your routing rules, you must identify a source network available to any specific interface card. The Aventail ExtraNet Server transparently detects installed network cards. This information appears at the Routing information dialog box.

ROUTING RULES

Routing rules specify what internal and external network traffic goes to which network interface cards (NIC) on a server. Routing rules work only for multihomed servers (a server with two or more installed network interface cards), and are not necessary for the server to properly function. However, you must properly configure multihomed servers in order to proxy chain and neutralize IP spoofing attacks.

The Aventail ExtraNet Server transparently detects installed network cards and available networks. This information appears in the Routing information dialog box where you can configure your routing rules.



Petitioner Apple Inc. - Ex. 1011, p. 55

Adding a route

At the Routing information dialog box,

1. Select the appropriate card that appears in the Interface: list box.
2. From the Available Networks pane, select the target network and move it to the Selected Source Networks pane.

Click **OK**. The new routing rule will appear in the Network Setup dialog box.

NOTE: *If you do not select a network but click* **OK***, all network traffic will route through the card displayed in the Interface: text box.*

Editing a route

At the Routing information dialog box, either:

1. Select a new network in the Available Networks pane.
2. Move that network to the Selected Source Networks pane
   -OR-
   Move the Selected Source Network to the Available pane,
   -AND/OR-
   Select a different card in the Interface: text box
3. Click **OK**. The edited routing rule will appear in the Network Setup dialog box.

Deleting a route

You can delete a route at the Network Setup dialog box.

Adding a routing rule

1. At the Policy Console, click Network Setup at the toolbar
   -OR-
   select View | Network Setup from the menu. Either action opens the Network Setup dialog box.
2. Click New... to open the Routing Information dialog box where you will configure your new routing setup.

Editing a routing rule

From the Policy Console menu,

1. select View | Network Setup...
   -OR-
   Click Network Setup on the tool bar. Either action opens the Network Setup dialog box.
2. At the Network Setup dialog box, Double-click in the white space of the Network Setup window,
   -OR-
   Right-click and select Edit... from the shortcut menu,
   -OR-
   Click Edit...to open the Routing Information dialog box where you can reconfigure your routing setup.

Petitioner Apple Inc. - Ex. 1011, p. 56

Deleting a routing rule

From the Policy Console menu,

1. select View | Network Setup...
   -OR-
   Click Network Setup on the tool bar. Either action opens the Network Setup dialog box.
2. At the Network Setup dialog box, select the rule you want to delete, and Right-click and select Delete from the shortcut menu,
   -OR-
   Click Delete. Either action removes the rule from the Network Setup dialog box.

Petitioner Apple Inc. - Ex. 1011, p. 57

Configuration File Format

INTRODUCTION

The configuration file `s5.conf` controls all aspects of the Aventail ExtraNet Server. By default, this file is located in `<prefix>/etc/s5.conf`, where `<prefix>` is the directory the Aventail ExtraNet Server was installed to (typically `/usr/local/aventail`). You can edit this file using a text editor.

The Aventail ExtraNet Server reads this configuration file the first time the server is started, and each time the process is restarted. This file contains all the policy information that the Aventail ExtraNet Server needs to handle a connection.

GENERAL SYNTAX

All entries in the configuration file are of the following format:

```
type name {
  key = value;
  key = value;
}
```

Case, new lines, and spacing are not significant, unless referring to an object name, or data within a quoted string. The name of the object is not significant, as long as it is unique within the configuration file.

The type of object determines which keys are within the block. The order of keys within the block is significant only in the Policy Object. In the Policy Object, the server reads each line, from top to bottom, until it makes a match; for a line to match, each entry within the line must match. For more information, refer to the “Policy” section.

DATA TYPES

There are five basic data types in the configuration file: tokens, booleans, integers, simple strings, and strings. The following object is used as an example in the definitions below:

```
installation @converted_installation
{
  comment = “Automatically converted from v2.x file:socks5.conf”;
  port = 1080;
  reversedns = TRUE;
}
```


Petitioner Apple Inc. - Ex. 1011, p. 58

Tokens

Tokens are the internal keywords that the parser recognizes. Tokens determine the type of data that can come after them. In the example above, `installation`, `comment`, `port`, `reversedns`, and `TRUE` are all tokens.

Tokens are not case-sensitive. Tokens should never be contained within quotation marks.

Booleans

Booleans can be either `TRUE` or `FALSE`. `TRUE` and `FALSE` are tokens that the parser recognizes internally. In the example above, `TRUE` is a boolean.

Booleans are not case-sensitive. Booleans should never be contained within quotation marks.

Integers

An integer can be any sequence of numbers. In the example above, `1080` is an integer.

Numbers cannot be negative, and floating point numbers are not allowed.

Simple Strings

A simple string must start with an "@" symbol, and must contain only alphabetic characters (a-z or A-Z), digits (0-9), and/or underscores (_). In the example above, `@converted_installation` is a simple string.

Strings

To avoid parse errors, a typical string is usually contained within quotation marks; this can reduce confusion between strings and tokens that otherwise appear identical.

In cases where quotation marks must be included within the string, basic escape mechanisms are available. To include a quotation mark within a string, type `'\''`. To include a literal backslash character, type `'\\'`. Placing any other character directly after a backslash (\) simply inserts that character. In the example above, `"Automatically converted from v2.x file:socks5.conf"` is a string in quotation marks.

COMMON ATTRIBUTES

Any object(s) can have the `comment = STRING` attribute included within the object body. This freeform string can contain information about the object. It is not parsed by the server or the graphic user interface (GUI) administration tool in any way. It is strictly for informational purposes.

Petitioner Apple Inc. - Ex. 1011, p. 59

ORDER OF OBJECTS

You must define all objects before using them. (This limitation will be removed in a future release of the Aventail ExtraNet Server.) The following example would result in a parse error because "`Second Group`" is used before it is defined.

```
group "First Group"
{
  local group "Second Group";
}
group "Second Group"
{
}
```

MODULES

All filters and authentication methods (except NULL) are defined in loadable modules so that, if desired, only the necessary functionality can be loaded into memory. Loadable modules also allow for in-house development of custom authentication methods or content filters.

You must complete three steps before a server will actually use a module. You must load the module, apply the module to a specific installation, and use the module in an access-control, authentication, or filter rule.

Loading a Module

You must load each module individually, in the module section. The module section also contains all configuration information for the module. The following example is used in the definitions below:

```
module "http_filter"
{
comment = "HTTP content filter";
filename = "modules/filters/http-filter.mod";
stub = "http_filter";
option "aventail" = "/usr/local/aventail/etc/avfilter.conf";
}
```

Parameter	Description
filename	Specifies where the loadable module can be found. This can be a fully qualified pathname (e.g., `/usr/local/aventail/modules/authentication/test.mod`), or relative to the installation directory (e.g., `modules/authentication/test.mod`).

Petitioner Apple Inc. - Ex. 1011, p. 60

Parameter	Description
stub	The unique identifier for the module. It is used to find all of the functions that the server needs. This is typically the name of the module, without the `.mod` suffix. All `'-'` characters will be converted to `'_'`.
option	All configuration information for the module includes any number of “option” statements. Options are module-specific.

Including a Module in an Installation

You must use a module in an installation before you can use it in the installation’s ACL, filter, or authentication rule. To include a module in an installation, use the “module” keyword. For example:

```
installation “Converted”
{
  module “http_filter”;
}
```

Referencing a Module in a Rule

Once you have loaded and included a module in an installation, any rule in that installation can reference the module. The type of module determines which referencing method to use.

- **Client-side Authentication:** Client-side modules are used only when proxy chaining, and do not need to be explicitly used in a rule. If the server you are chaining to requires authentication, all configured authentication methods will be offered in the negotiation phase, and the remote server will select the most appropriate method.
- **Server-side Authentication:** Server-side modules are used to force clients to authenticate in a certain way. Authentication methods are referenced by a short, unique string, which maps to a specific authentication method. The Aventail ExtraNet Center includes the following authentication methods by default: SSL, Username/Password, CHAP, CRAM, and Null. Other methods can be installed by third parties or local system administrators. If you are unsure of which authentication methods are available in your installation, contact your local system administrator.

  To configure the server to require a certain authentication method, include that method in an authentication rule and, if necessary, in any access control or filtering rules that might require greater control than an authentication rule can provide.
- **Content Filters:** Content filters are referenced by a short, unique string, which maps to a specific filter method. Content filters are used only in filter rules. The Aventail ExtraNet Center includes the following filters by default: http, http-forwarder, and print. Other methods can be installed by third parties or local system administrators. If you are unsure of which filters are available in your installation, contact your local system administrator.

Petitioner Apple Inc. - Ex. 1011, p. 61

- **Access Control:** Access-control modules do not need to be explicitly used in a rule. Access-control modules are used in the order in which you load them. If a module refuses a connection, none of the subsequent modules will be consulted.

  The Aventail ExtraNet Center does not ship with any access-control modules by default; however, other methods can be installed by third parties or local system administrators. If you are unsure of which access-control methods are available in your installation, contact your local system administrator.

DEFINING USERS AND GROUPS

You do not need to explicitly define users and groups before using them in a rule or group definition; the users and groups are self-describing.

The standard user/group notation is "`backend:name`" where "`backend`" is a string that uniquely identifies a backend where the actual authentication information is stored, and "`name`" is the user/group name. Specifying the special backend "`any`" means that any backend should match the username.

To use a user or group in a rule or group, use the group or user keywords. For example:

```
access permit @ac10
{
   .
   .
   .
   user “unix:root”;
   group “unix:wheel”;
   user “unix:dhdore”;
   user “any:ichabod”;
}
```

When using the same set of users in many rules, it is easier to put them into a group locally and use those groups in the rules. The "group" object defines a local group. You can include users, groups, and other local groups in a local group. You can also mix and match backends. For example:

```
group “Special Users”
{
   user “unix:root”;
   group “unix:wheel”;
   user “unix:dhdore”;
   user “any:ichabod”;
}
access permit @ac11
{
   .
   .
   .
   local group “Special Users;
}
```


Petitioner Apple Inc. - Ex. 1011, p. 62

DEFINING NETWORKS

To define networks and hosts, use the network object. There are four types of networks; they all follow the same pattern in the configuration file:

```
network <TYPE> “name
{
  key1 = value 1;
  key2 = value 2;
}
```

The <TYPE> determines which keys are valid.

- **Domain:** This type of network is used to match an entire domain of machines. The domain keyword is used to define the domain. For example:

  ```
  network domain “GNU Domain”
  {
     domain = “gnu.org”;
  }
  ```

  Any machine name that ends with the domain matches. Examples of matches and mismatches:

  `www.aventail.com` **IS** in `.aventail.com`
  `www.aventail.com` **IS NOT** in `.bob.aventail.com`
  `patrick.in.aventail.com` **IS** in `.aventail.com`

- **Host:** This matches a specific machine. You can match the host machine with either the IP address or the hostname keywords. The IP address should be in dotted-decimal notation, and the hostname should be a string. For example:

  ```
  network host “Mythical machine”
  {
     ipaddress = “123.456.7.8”;
  }
  network host “Another Mythical machine”
  {
     hostname = “test.test.ick.bin.org”;
  }
  ```

  Hostname comparisons are case-insensitive; therefore, `WWW.AvEnTAiL.com` matches `www.aventail.com`, and vice versa.

- **Subnet:** You can define an entire subnet with this type of network. The IP address and netmask keywords recognized and should be in the standard dotted-decimal notation. For example:

  ```
  network subnet “123.456.7.8.xxx Subnet”
  {
  ipaddress = “123.456.7.1”;
  netmask = “255.255.255.0”:
  }
  ```

- **Range:** Occasionally, a grouping of machines cannot easily be described with a subnet mask. A network can also be a consecutive range of IP addresses.

Petitioner Apple Inc. - Ex. 1011, p. 63

The from and to keywords specify the beginning and end of a range in dotted-decimal notation. For example:

```
network range “Subrange of 123.456.7.xxx”
{
from = “123.456.7.5”;
to = “123.456.7.25”;
}
```

The range is inclusive, which means that the endpoints are included in the range. In the example above, “`123.456.7.5`” and “`123.456.7.25`” would match the specified range.

DEFINING SOCKS SERVERS

SOCKS server definitions are used in proxy chaining rules. The following table explains the attributes that you can specify.

Parameter	Description
hostname	The hostname of the SOCKS server. If you specify the hostname, you do not need to specify the IP address.
ipaddress	The hostname of the SOCKS server in dotted-decimal notation. If you specify the IP address, you do not need to specify the hostname.
port	The port number that the server is listening on.
version	The SOCKS protocol version the server speaks. Valid version numbers are “4” and “5.”

An example of a SOCKS server definition is:

```
server “slow”;
{
  hostname = “slow”;
  port = 1080;
  version = 5;
}
```

RULES

There are five types of rules that determine how a connection will be handled: Authentication, Access-control, Filters, Routing Entries, and Proxy-chaining. Rules are evaluated in the order in which you list them in the installation object. The server applies the first matching rule to the connection, then the second matching rule, and so on.

Petitioner Apple Inc. - Ex. 1011, p. 64

Rule	Description
Authentication Rule	Determines how a client will be allowed to authenticate to the server.
Access-control Rule	Specifies the class(es) of connection allowed through the server. Connections can be accepted or rejected.
Filter Rule	Determines whether or not a content filter needs to be applied to the data stream. This is the final decision made before starting to proxy data.
Routing Entries	Specifies which network interface each machine can use.
Proxy-chaining Rule	Controls which traffic (if any) will be directed through subsequent servers. This is typically used for access to partners' networks where individual users in the company do not have accounts but the company as a whole does.

Common Attributes of Rules

You can use the following attributes in any of the rule types. If you specify multiple networks, network groups, users, or groups, this becomes an "OR" operation. For example, the user could be "Deb" *or* "Dale" *or* "Eric," etc.

Attribute	Description
enabled	Controls whether or not the rule will actually be considered when the server looks for matches. If FALSE, it will be skipped completely. This is useful for temporarily disabling a certain set of access rights.
network source name	Specifies that the user's connection must originate from the network source for the rule to apply.
network group source name	Specifies that the user's connection must originate from the network source for the rule to apply.
source services	Specifies that the user's connection must originate from any of the listed ports for the rule to apply. You can list either single services or ranges of services.
methods	Specifies that the user must authenticate using one of the methods listed for the rule to apply. For information about which authentication modules are supported, refer to "Authentication."

Petitioner Apple Inc. - Ex. 1011, p. 65

Attribute	Description
keylength	Specifies that the session must be encrypted with a key of a certain minimum length for the rule to apply. Valid key lengths are 0, 40, 56, or 128 bits.
user backend	Specifies that the authenticated user must be the named user according to the backend in order for the rule to apply.
group backend	Specifies that the authenticated user must be in the named group according to backend in order for the rule to apply.
local group name	Specifies that the authenticated user must be in the locally defined group name in order for the rule to apply.
DAY	One of Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday. The right-hand side is a list of one or more time ranges, in 24-hour format. The granularity of the times is on the half hour only. Time ranges are inclusive.
startdate	Start date in mm/dd/yyyy notation.
enddate	End date in mm/dd/yyyy notation.
starttime	Start time in hh:mm notation.
endtime	End time in hh:mm notation.

Authentication

The methods keyword determines which authentication method(s) will be accepted from different networks. There are no new keywords available for this object type. For example:

```
authentication @ac10
{
  enabled = TRUE;
  network source = “Anywhere”;
  methods = “password “ “cram” “ssl”;
}
```

Access Control

Access-control rules determine who can go where, and when, through the server. An access-control rule specifies, in the object definition, whether it will permit or deny access to the listed resources. Each entry on the line must match for the entire line to match. For example:

```
access permit @ac10
{
  enabled = TRUE;
```


Petitioner Apple Inc. - Ex. 1011, p. 66

```
  network source  “Anywhere”;
  network destination “Anywhere”;
}
access deny @ac11
{
  enabled = TRUE
  network source “Anywhere”;
  network destination “Anywhere”;
}
```

You can apply the following new attributes to access-control rules.

Attribute	Description
commands	Specifies that the user can use only the commands listed. Recognized commands are “connect,” “bind,” udp,” “ping,” or “traceroute.” The commands correspond to the SOCKS commands for proxying different types of traffic.
network destination name	Specifies that the user must be attempting to reach the network name for the rule to apply.
network group destination name	Specifies that the user must be attempting to reach any of the networks in name for the rule to apply.
source services	Specifies that users must be attempting to reach any of the listed ports for the rule to apply. You can list either single services or ranges of services.

Filters

Filter rule objects can have any of the common attributes and access-control attributes, and include the following attributes:

- **`module = filtername;`**

  This attribute specifies the name of the filter to apply if the connection matches this rule. For more information on content filters, refer to “Filters.”

- **`filter @filter0`**

```
{
   enabled = TRUE
   module = “http”;
   SUNDAY = 00:00-24:00
   MONDAY = 00:00-24:00
   TUESDAY = 00:00-24:00
   WEDNESDAY = 00:00-24:00
   THURSDAY = 00:00-24:00
   FRIDAY = 00:00-24:00
   SATURDAY = 00:00-24:00
}
```


Petitioner Apple Inc. - Ex. 1011, p. 67

Routing Entries

On machines with multiple network interfaces (i.e., IP addresses), it is important to ensure that the machines use certain network interfaces in conjunction with certain addresses. This prevents IP spoofing (where machines outside the network pretend to be machines inside the network) by ensuring that inside machines use the inside network and outside machines use the outside network. This is also used by SOCKS servers in determining which network interface to bind on when accepting a BIND request, or when issuing a SENDTO request. If no entry matches, the SOCKS server uses INADDR_ANY to bind, and a connection can be received on any interface. Single-homed hosts do not need routing entries; they are necessary only when machines have more than one network interface. The format for the routing-entry object is:

```
card = string;
```

Proxy Chaining

Proxy-chaining entries describe the addresses of SOCKS proxy servers. There lines tell the server how to contact a given host. If no lines match a host, the server contacts the host directly. The format for the proxy-chaining object is:

```
noproxy = boolean;
server = name;
```

INSTALLATION

The following table describes the attributes of the installation object.

Attribute	Description
port	Specifies the port number that the server should listen on for incoming connections.
identd	Specifies whether to use the IDENTD protocol when using NULL authentication. (This attribute is not supported in v3.0.)
reversedns	Specifies whether to attempt reverse DNS. This is a legacy option. The server does reverse DNS only when necessary (e.g., when a rule needs to check it against a domain-based network, etc.).
udprestrict	Specifies whether the server should accept UDP traffic from anyone, or only from machines that it has previously talked to.
udpclientsport	Specifies whether the server should try to use the same port number on its external interface that the client has used internally. This can improve the performance of some UDP applications.
udpbind	This attribute is no longer used.

Petitioner Apple Inc. - Ex. 1011, p. 68

Attribute	Description
timeout	Specifies how long idle connections are allowed to stay active. This attribute is used in conjunction with the time-unit attribute (below).
timeunit	Used in conjunction with the timeout attribute (above) to specify how long idle connections are allowed to stay active.
secout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `security.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
sysout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `system.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
miscout	Specifies where to log security warnings to. SYSTEM refers to the system logger (syslog under Unix, Event-Viewer under Windows NT). LOGFILE refers to the `misc.log` file under logroot. LOGTOOL refers to the Logging Utility application under Windows NT. For more information, see "Logging."
seclevel	Specifies the error level for logging security messages. For more information, refer to "Logging."
syslevel	Specifies the error level for logging system messages. For more information, refer to "Logging."
misclevel	Specifies the error level for logging miscellaneous messages. For more information, refer to "Logging."
logroot	Specifies the directory that will contain the log files.
auditlog	Specifies whether to keep an audit log of all connections processed by the server.
auditpath	Specifies the directory that will contain the audit files. Three files are created in this directory: *accounting*, which contains the main audit trail; *security*, which contains additional security information; and *errors*, which contains information about failed connections (due to network errors, etc.).

Petitioner Apple Inc. - Ex. 1011, p. 69

Attribute	Description
auditformat	Specifies which format to log the auditing information in. Currently supported formats are the WebTrends Enhanced Log Format (WELF) and a flat text file specific to Aventail, which is easily imported into spreadsheets or databases.
buffersize	Specifies how much data to attempt to read from the network at one time. Larger sizes may improve throughput, but will increase memory usage.
maxchildren	Maximum number of connections to allow at any one time. The license should do this automatically.
servicenames	Specifies whether to look up service names to use in logging messages and audit files.
backlog	Specifies how many pending connections to allow to "stack up." The default value is "5." On some versions of Unix, the TCP/IP stack ignores this value. Once the maximum allowable number of connections is in the queue, the server will reject new connections.
pidfile	*(Unix only)* Specifies where to store the process ID. This file is used by the stopsocks script. You usually do not need to specify this attribute.
ipspoofing	Specifies whether to watch for IP spoofing attacks, and reject potentially bad connections. If this option is activated (TRUE), the server will reject any connection that originates from a network interface that it would not use in talking to that host. In complicated network setups, this can cause problems, and should probably not be activated (set to FALSE).
alertfrequency	
alertthreshold	
traceroute program	Specifies which program to execute when a "traceroute" command is proxied. This should be the executable name by itself, or a fully qualified pathname to the executable (if it is not in the default path for the user the server is running as).
pingprogram	Specifies which program to execute when a "ping" command is proxied. This should be the executable name by itself, or a fully qualified pathname to the executable (if it is not in the default path for the user the server is running as).

Petitioner Apple Inc. - Ex. 1011, p. 70

Attribute	Description
nlsdirectory	Specifies where to find the NLS catalogs for the server. In most cases, this attribute should not be set. The server will automatically determine where the catalogs are installed.
module module_name	Use the module module_name in this installation. This means that the module will be loaded and available for use in any rules in the Policy section (see below).

POLICY

The policy object is where you arrange all of the rules and give them a specific ordering. The ordering of similar attributes is important, and can significantly affect the policy enforced by the server. Be sure to order or reorder rules carefully.

The following table describes the additional attributes that are valid in a policy object.

Attribute	Description
interface string	Imports the routing rule named "*string*" into the current policy.
authentication string	Imports the authentication rule named "*string*" into the current policy.
proxy string	Imports the proxy chaining rule named "*string*" into the current policy.
filter string	Imports the filter rule named "*string*" into the current policy.
access string	Imports the access-control rule named "*string*" into the current policy.

An example of a policy object is:

```
policy "Converted"
{
  interface @route0;
  authentication @auth0;
  proxy @proxy0;
  proxy @proxy1;
  filter @filter0;
  access @ac10;
  access @ac12;
}
```


Petitioner Apple Inc. - Ex. 1011, p. 71

LOGGING

Logging is an essential part of maintaining server function. With logging, you can track user activity, diagnose failed connections, repair system failures, and configure the logging output for Aventail or WebTrends formats.

Logging options include three logging methods, eight levels of information, four output options, and two output formats.

Log Methods

There are three log methods: Security, System, and Miscellaneous. When logging server activity, select one of the three methods.

- **Security:** Security information consists of failed authentication attempts and methods. When logging to LOGFILE, the filename is `security.log`.
- **System:** System information identifies and displays network problems as they affect the ExtraNet Server. Examples of network problems include low memory, timing out, a SOCKS server crash, etc. When logging to LOGFILE, the filename is `system.log`.
- **Miscellaneous:** Miscellaneous information consists of everything else not included in the Security and System methods. When logging to LOGFILE, the filename is `misc.log`.

Log Levels

There are eight log levels: Fatal, Error, Warning, Information, Verbose, Debug1, Debug2, and Debug3. When logging server activity, select one of the eight methods.

NOTE: *Processing large amounts of information by logging at the Verbose level or higher can impact the server's performance for brief periods of time.*

NOTE: *Logging at a certain level includes all levels below that level as well. For example, logging at the Warning level includes Fatal and Error messages as well.*

Log Level	Description
Fatal	Fatal error information only.
Error	Critical error information only.
Warning	Non-critical warning information.
Information	Detailed logging information.

Petitioner Apple Inc. - Ex. 1011, p. 72

Log Level	Description
Verbose	More detailed logging information than the Information level, but not as detailed as the Debug-level information.
Debug1, Debug2, Debug3	Debugging levels of increasing verbosity. This can cause large amounts of data to be written, and should be used only when troubleshooting.

Log Output Options

There are three log-output options: SYSTEM, LOGTOOL, and LOGFILE. You can specify multiple output options at once.

- **SYSTEM:** Selecting this log-output option will cause logging information to output to the system logger. Under Unix, the system logger is syslog, and under Windows NT it is the Event Viewer Application Log. Under Windows NT, the server will always log startup information to the Event Viewer.
- **LOGTOOL:** This option is currently valid only under Windows NT. The Logging Tool is the dynamic logging tool for all Aventail ExtraNet Server activity. The Logging Tool can dynamically filter out certain types of log messages and is useful for debugging quickly without having to bring the server up and down to change log levels.
- **LOGFILE:** Selecting this log-output option will cause logging information to log to the appropriate flat file in the logroot directory.

Auditing

The auditing subsystem tracks where users are going, and how much bandwidth they are using. Auditing can be useful for fine-tuning policy if certain types of traffic start using too much bandwidth.

Audit Log Types

There are three audit log types: Error Audit Log, Accounting Audit Log, and Security Audit Log.

- **Error Audit Log:** The Error Audit Log records failed connections that result from system or hardware lapses or failures.
- **Accounting Audit Log:** The Accounting Audit Log records successful system and authentication connections.
- **Security Audit Log:** The Security Audit Log records failed connections that result from authentication lapses or failures.

Information Types

Log entries can contain varying amounts of information, depending on the type of log and the connection status of each entry. Log entries are in a text-only, space-delimited format (with date and time within quotation marks). Log entries allow administrators to track

- Traffic date and time
- Source and destination

Petitioner Apple Inc. - Ex. 1011, p. 73

- Connection duration
- Authentication methods
- Commands
- Bytes received
- Exit status

Output Formats

The two valid output formats are the Aventail format and the WebTrends Enhanced Log Format (WELF).

- **Aventail:** This is a flat text file format specific to Aventail, which is easily imported into spreadsheets or databases. Below is an example entry format.

  ```
  bob.bp.aventail.com:1234 null dhdore “15 May 1998
  09:20:57” v4 connect www.gnu.org:http 0 19252 1195 38
  ```

- **WebTrends Enhanced Log Format (WELF):** With WebTrends products, you can save, FTP, or e-mail reports in Microsoft Word, Microsoft Excel, HTML, text, or comma-delimited text formats. For more information about WebTrends, contact WebTrends at `http://www.webtrends.com`.

Petitioner Apple Inc. - Ex. 1011, p. 74