Gauntlet® for IRIX®
Netperm Table Reference Guide

Version 4.1

Document Number 007-3822-003

CONTRIBUTORS

Written by Renate Kempf with updates by Terry Schultz based on material from Trusted Information Systems, Inc.
Production by Heather Hermstad and Amy Swenson
Engineering contributions by Jessica Humphreys, Ed Mascarenhas, Dj Padzensky, and Mayank Vasa.
St. Peter's Basilica image courtesy of ENEL SpA and InfoByte SpA. Disk Thrower image courtesy of Xavier Berenguer, Animatica.

Gauntlet® for IRIX® Netperm Table Reference Guide
Document Number 007-3822-003

Contents

List of Tables xix

About This Guide xxi
Audience xxi
Structure of This Guide xxi
Conventions xxii

1. Understanding the Netperm Table 1
Policy Rules 2
Application-Specific Rules 2
Rules for Proxies 2
Gauntlet Applications and the Netperm Table 3
How the Netperm Table is Used 3

2. Netperm Table Setup 5
Precedence in Netperm Tables 6
Netperm Table Format 6
Comments in Netperm Tables 7
Netperm Table Keywords 7
Attributes in Netperm Tables 9

3. Policies and Services 11
Creating New Policies 11
How to Create a New Policy 11
Example for Creating a New Policy 12
Adding Proxy Services 13
Denying Proxy Services 14

Denying Services by Network or Host 14
Denying Access From a Host or Network 15
Denying Access by Proxy 15
Denying Access From a Host or Network 15
Denying Access to a Host, Network, or Proxy 16
Denying Access by Proxy 16
Denying General Access to a Host or Network 16
Controlling Services by User, Group, or Time 16
Controlling Services by User or Group 17
Controlling Services by Operation 17

4. Attribute Reference 19
accept-count 20
Syntax 20
Example 20
admin-user 21
Syntax 21
Example 21
Gauntlet Firewall Manager 21
agent 22
Syntax 22
Example 23
Gauntlet Firewall Manager 23
anon-user 23
Syntax 24
Example 24
authenticate (all but pcxdpp) 24
Syntax 25
Example 25
Gauntlet Firewall Manager 25
authenticate (pcxdpp only) 25
Syntax 26
Example 26

authserver 27
Syntax 27
Example 27
Gauntlet Firewall Manager 27
authtype 28
backend 28
Syntax 28
Example 28
badadmin 29
Syntax 29
Example 29
Gauntlet Firewall Manager 29
baddir 30
Syntax 30
Example 30
Gauntlet Firewall Manager 30
badsleep 31
Syntax 31
Example 31
bind-address 32
Syntax 32
Example 33
bind-inside 33
Syntax 34
Example 34
block 34
Syntax 35
Example 35
buffer-size 35
Syntax 36
Example 36

check-server-ip 36
Syntax 37
Example 37
child-limit 37
Syntax 38
Example 38
Gauntlet Firewall Manager 38
circuitexec 38
Syntax 39
Example 39
Gauntlet Firewall Manager 39
circuitsperuser 39
Syntax 40
Example 40
Gauntlet Firewall Manager 40
circuit-timeout 40
Syntax 41
Example 41
Gauntlet Firewall Manager 41
client 41
Syntax 42
Example 42
Gauntlet Firewall Manager 42
connect-timeout 43
Syntax 43
Example 43
Gauntlet Firewall Manager 43
content-failunsafe 44
Syntax 44
Example 44

content-ftpcheck 45
Syntax 45
Example 45
Gauntlet Firewall Manager 45
contentscan-msg 46
Syntax 46
Example 46
Gauntlet Firewall Manager 46
cvp-handling 47
Syntax 47
Example 47
Gauntlet Firewall Manager 47
cvp-server 48
Syntax 48
Example 48
Gauntlet Firewall Manager 48
cyber_masks 49
Syntax 49
Example 50
Gauntlet Firewall Manager 50
data-port 51
Syntax 51
Example 51
database (authsrv only) 52
Syntax 52
Example 52
database (pcxdpp only) 52
Syntax 53
Example 53
database (pop3-gw only) 53
Syntax 54
Example 54
Gauntlet Firewall Manager 54

denial-msg 55
Syntax 55
Example 55
Gauntlet Firewall Manager 55
denydest-msg 56
Syntax 56
Example 56
Gauntlet Firewall Manager 56
deny-spam 57
Syntax 57
Example 57
destination 58
Syntax 58
Example 58
Gauntlet Firewall Manager 59
directory (gui, info-gw, smap and smapd only) 59
Syntax 59
Example 59
Gauntlet Firewall Manager 60
directory (all others) 60
Syntax 60
Example 60
Gauntlet Firewall Manager 61
display 61
Syntax 61
Example 62
exec 62
Syntax 62
Example 63
extended-permissions 63
Syntax 63
Example 64
Gauntlet Firewall Manager 64

feature 64
Syntax 1 64
Example 65
Gauntlet Firewall Manager 65
Syntax 2 65
Example 66
Gauntlet Firewall Manager 66
force_source_address 66
Syntax 66
Example 67
Gauntlet Firewall Manager 67
forward 67
Syntax 68
Example 68
forward (authenIP only) 68
Syntax 69
Example 71
Gauntlet Firewall Manager 71
function 72
Syntax 72
Example 74
Gauntlet Firewall Manager 74
groupid 75
Syntax 75
Example 75
Gauntlet Firewall Manager 75
handoff 76
Syntax for ftp-gw 76
Example 76
Gauntlet Firewall Manager 76
Syntax for http-gw 77
Example 77
Gauntlet Firewall Manager 77

header 78
Syntax 78
Example 79
help-msg 79
Syntax 79
Example 80
Gauntlet Firewall Manager 80
hosts (authsrv only) 80
Syntax 80
Example 81
hosts (all but authsrv) 81
Syntax 81
Example 82
Gauntlet Firewall Manager 82
if-inside 83
Syntax 83
Example 83
Gauntlet Firewall Manager 83
if-outside 84
Syntax 84
Example 84
Gauntlet Firewall Manager 85
keepalive-timeout 85
Syntax 85
Example 85
Gauntlet Firewall Manager 86
local 86
Syntax 86
Example 87
Gauntlet Firewall Manager 87
local-domain 87
Syntax 88
Example 88

log 89
Syntax 89
Example 90
Gauntlet Firewall Manager 90
log (smap only) 91
Syntax 91
Example 91
manager 92
Syntax 92
Example 92
Gauntlet Firewall Manager 92
maxbad 93
Syntax 93
Example 93
maxbytes 94
Syntax 94
Example 94
maxchildren 95
maxrecip 95
Syntax 95
Example 95
maxsessions 96
Syntax 96
Example 96
NetShow 97
Syntax 97
Example 97
Gauntlet Firewall Manager 97
nobogus 98
Syntax 98
Example 98

operation 99
Syntax 99
Example 100
Gauntlet Firewall Manager 101
ourname 101
Syntax 101
Example 102
password change 102
Syntax 102
Example 103
Gauntlet Firewall Manager 103
password-timeout 103
Syntax 104
Example 104
peer-net 104
Syntax 105
Example 105
Gauntlet Firewall Manager 105
permit-relay 105
Syntax 106
Example 106
pop-server 107
Syntax 107
Example 107
Gauntlet Firewall Manager 107
port 108
Syntax 108
Example 109
Gauntlet Firewall Manager 109
ports 109
Syntax 110
Example 110

printer 111
Syntax 111
Example 111
Gauntlet Firewall Manager 112
prompt 112
Syntax 112
Example 112
Gauntlet Firewall Manager 112
proxy 113
Syntax 113
Examples 113
Gauntlet Firewall Manager 114
quarantine-dir 114
Syntax 114
Example 114
Gauntlet Firewall Manager 115
RealAudio 115
Syntax 115
Example 115
Gauntlet Firewall Manager 116
require-source 116
Syntax 116
Example 116
securidhost 117
Syntax 117
Example 117
Gauntlet Firewall Manager 117
send-broken-post-requests 118
Syntax 118
Example 118
Gauntlet Firewall Manager 118

sendmail 119
Syntax 119
Example 119
Gauntlet Firewall Manager 119
server 120
Syntax 120
Example 121
Gauntlet Firewall Manager 121
shellfile 121
Syntax 122
Example 122
snmp-manager 122
Syntax 122
Example 123
Gauntlet Firewall Manager 123
system-contact 123
Syntax 124
Example 124
Gauntlet Firewall Manager 124
system-location 124
Syntax 125
Example 125
Gauntlet Firewall Manager 125
system-name 126
Syntax 126
Example 126
Gauntlet Firewall Manager 126
tempdir 127
Syntax 127
Example 127

timeout 128
Syntax 128
Example 128
Gauntlet Firewall Manager 128
tmp-directory 129
Syntax 129
Example 129
transparency 130
Syntax 130
Example 130
unknown 131
Syntax 131
Example 131
url 132
Syntax 132
Example 133
Gauntlet Firewall Manager 133
url-filter 133
Syntax 134
Example 134
Gauntlet Firewall Manager 134
userid 134
Syntax 135
Example 135
Gauntlet Firewall Manager 135
user-servers 135
Syntax 136
Example 136
Gauntlet Firewall Manager 136
user-timeout 137
Syntax 137
Example 137
Gauntlet Firewall Manager 137

VDOLive 138
Syntax 138
Example 138
Gauntlet Firewall Manager 138
virtual-net 139
Syntax 139
Example 140
Gauntlet Firewall Manager 140
wakeup 140
Syntax 140
Example 141
Gauntlet Firewall Manager 141
welcome-msg 141
Syntax 141
Example 142
Gauntlet Firewall Manager 142
work_time 142
Syntax 143
Example 143
Gauntlet Firewall Manager 143
xforwarder 144
Syntax 144
Example 144
Gauntlet Firewall Manager 144
xgateway 145
Syntax 145
Example 145
Gauntlet Firewall Manager 145

5. Keyword Reference 147
ahttp-gw 147
aol-gw 147
authenIP 148
authsrv 148

ck-gw 149
cserve-gw 150
finger 150
ftp-gw 151
gopher-gw 152
gui 152
http-gw 153
info-gw 154
ldap-gw 154
lnotes-gw 155
login-sh 155
lp-gw 155
mbase-gw 156
mmp 156
mssql-gw 157
netacl 157
netconfig 158
NetShow 158
nntp-gw 158
pcxdpp 159
plug-gw 159
pop3-gw 160
radm 160
RealAudio 160
rlogin-gw 161
rsh-gw 162
smap 162
smapd 163
snmpd 163
snmp-gw 164
ssl-gw 164
strmwrks-gw 165
syb-gw 165

tn-gw 165
VDOLive 166
whois 167
x-gw 167

Index 169

List of Tables

Table 2-1 Common Keywords and Associated Applications 7

About This Guide

The *Netperm Table Reference Guide* describes the Gauntlet Firewall network permissions (netperm) table and explains how to use it.

Note: Trusted Information Systems, the manufacturer of the Gauntlet product, recommends using the Gauntlet Firewall Manager graphical user interface to configure your firewall. However, if you have an unusual configuration or need to configure an option that you cannot set through the Gauntlet Firewall Manager, the netperm table is available.

Audience

This reference guide is intended for firewall administrators. It assumes familiarity with UNIX system administration, networking, network administration, and basic firewall concepts. System administrators should be familiar with TCP/IP, domain name service, sendmail, and router configuration.

Structure of This Guide

This reference guide has the following chapters:

- Chapter 1, "Understanding the Netperm Table," describes the netperm table, including policy and application-specific rules.
- Chapter 2, "Netperm Table Setup," explains how to modify the netperm table and explains netperm table syntax.
- Chapter 3, "Policies and Services," explains how to create new policies, add or deny proxy services, deny services by network or host, and control services by user, group, or time.

- Chapter 4, “Attribute Reference,” lists all netperm table attributes and provides the information you need to use them.
- Chapter 5, “Keyword Reference,” lists each netperm table keyword and the attributes it can use.

Conventions

These type conventions and symbols are used in this guide:

Italics— executable names, filenames, IRIX commands, manual/book titles, new terms, utilities, variable command-line arguments, and variables to be supplied by the user in code examples, and syntax statements.

`Fixed-width type`—Code examples, prompts, and onscreen text.

`Bold fixed-width type`—User input, including keyboard keys, printing and nonprinting.

> (Single angle bracket)—Indicates “downward” movement in the graphical user interface. For example, “Environment > Firewall Access tab > UserName” means “In the Environment window, click the Firewall Access tab, then choose User Name.”

Chapter 1

Understanding the Netperm Table

The netperm table (*/usr/local/etc/netperm-table*) contains configuration information for the Gauntlet Firewall. The kernel, proxies, and other applications read configuration information from this table.

The recommended method of configuring the Gauntlet Firewall is through the Gauntlet Firewall Manager graphical user interface. Edit the netperm table only if you:

- Have an unusual configuration, such as four network interface cards
- Need to configure an option that you cannot set through the Gauntlet Firewall Manager

Changes you make to the netperm table may conflict with the settings generated by the Gauntlet Firewall Manager.

This chapter describes the Gauntlet Firewall's network permissions (netperm) table by discussing the different types of rules:

- "Policy Rules" on page 2
- "Application-Specific Rules" on page 2

Policy Rules

Policies are collections of general configuration information. Policies allow you to closely map your security requirements to the configuration of your Gauntlet firewall. Gauntlet configuration policies often include information such as:

- Types of proxies that the firewall can start
- Permitted (or denied) destinations for requests
- Authentication requirements

The source address of the request is the basis for a policy. You define policies for a set of hosts. You can easily use the same set of rules for a group of hosts by creating a generic policy describing what these hosts can and cannot do.

Application-Specific Rules

In addition to policy rules, the netperm table includes configuration information for proxies and other firewall applications, such as:

- Userid and groupid under which a proxy should run
- Directories that the proxies should use as their root directories
- Messages that proxies should display when denying or accepting requests
- Length of idle time before the proxies should terminate the connection
- More specific lists of permitted and denied destination networks for a particular proxy

Rules for Proxies

Suppose, for example, that the SMAP proxy reads the netperm table and determines the userid under which it should run and the directory into which it should place mail. The TELNET proxy reads the netperm table to determine how long a session must be idle before it disconnects the session. The specific configuration options for each proxy are described in Chapter 4, “Attribute Reference.”

You can also include rules to permit or deny a particular service for requests to specific addresses or networks. For example, you can configure the HTTP proxy to deny requests to a particular host or network. All of the other proxies, such as the smapd server, continue to use the generic policy and send information to that site, while the HTTP proxy denies requests to that site.

Because the proxies and applications read the netperm table from top to bottom and stop on the first match, you must put proxy-specific rules before the generic policies. When the relevant proxy parses the configuration information, it uses the proxy specific rule rather than the more general policy rule.

For example, the FTP proxy includes a specific rule that denies requests to the destination ftp.bigu.edu. You have created a policy for untrusted hosts, near the bottom of the netperm table, which includes a rule that allows all proxies and applications to send to any destination. Because the more restrictive rule is above the generic policy in the netperm table, the FTP proxy uses the restrictive rule and denies requests to ftp.bigu.edu.

Gauntlet Applications and the Netperm Table

Other Gauntlet applications such as the authentication server and the IP screening utility also read configuration information from the netperm table. For example, configuration information in the netperm table tells the authentication server how many incorrect login attempts to allow before disabling an account.

How the Netperm Table is Used

As part of the startup process, a proxy or application reads the netperm table looking for applicable configuration rules. It parses the table from top to bottom, looking for rules that match its name. It also matches wildcard rules that apply to all applications. For example, the TELNET proxy (tn-gw) looks for rules that match tn-gw and *.

The proxy goes through these steps:

1. It uses the rules to determine if it can accept the request from the source address.
2. It determines whether the requested service is an explicitly permitted service.
    - If the request is not permitted, the proxy denies it.
    - If the request is permitted, the proxy uses the other rules to determine whether it has to authenticate the request, and whether it can send the request to the specified destination.

The application also finds and uses rules for itself in the netperm table.

For example, using the default untrusted policy, the TELNET proxy allows TELNET requests from any outside network to any destination. The proxy also uses the untrusted policy to determine that it has to authenticate the user and it gets information about which server it should use to authenticate the user.

Chapter 2

Netperm Table Setup

This chapter provides important information about netperm table setup. You can modify the netperm table using your favorite text editor.

Note: Be sure to make a backup copy of the original netperm table. Do *not* edit in the section labeled Computer Generated Area (between the `#BEGIN WARNING` and `#END WARNING` marks).

With a few exceptions, you do not need to restart the proxies for the changes to take effect. Each time the proxies start new processes, they check the last modification time of the netperm table. If the time has changed, the proxies reread the netperm table. However, there are several proxies that must be restarted when you make changes to certain attributes. Chapter 4, "Attribute Reference," lists each attribute and notes whether restart is necessary.

This chapter contains information on the netperm table syntax in the following sections:

- "Precedence in Netperm Tables" on page 6
- "Netperm Table Format" on page 6
- "Comments in Netperm Tables" on page 7
- "Netperm Table Keywords" on page 7
- "Attributes in Netperm Tables" on page 9

Precedence in Netperm Tables

Applications and proxies read the rules from the top of the table to the bottom. They use the first rule that applies for a particular attribute. If there are multiple rules in the table that could apply for an attribute, the application uses the first one it finds.

For example, a netperm table attribute contains the following rule:

```
smapd: userid uucp
```

and later in the file contains the rule:

```
smapd: userid mail
```

When *smapd* parses the netperm table, it uses the first rule it finds, and runs as the user uucp.

Netperm Table Format

Each line in the netperm table contains a separate configuration rule in the format:

keyword: *attribute valuelist*

where:

- *keyword* indicates the application to which the rule applies. The wildcard (*) indicates the rule is valid for all applications and proxies. A comma-separated list of multiple keywords indicates the rules applies to all of the applications in the list. The keyword usually matches the name of the service or the value of the **-as** flag in the startup script.
- *attribute* is a configuration parameter for the application or proxy.
- *valuelist* is the value for the specific configuration parameter. Some attributes allow multiple values.

A rule must fit on a single line. The length of a line varies by operating system, but is usually around 1,024 bytes. There is no provision for continuing lines.

The keyword(s), attribute, and value list can be separated by spaces or tabs.

Comments in Netperm Tables

A hash mark (#) at the beginning of a line indicates a comment. Applications ignore any text between the hash mark at the beginning of the line and the end of the line. If the hash mark appears later in the line, applications treat the hash mark as a normal character. Applications treat the following line as a comment:

```
#set timeout to five minutes
```

Applications treat the following line as invalid syntax:

```
tn-gw: timeout 3000 #set timeout to five minutes
```

Note: Some default comments in the netperm table include information for the substitution driver. They begin with `#%subs-start` and end with `#%subs-end`. Do *not* delete these lines.

Netperm Table Keywords

The following table lists some common keywords for proxies and other applications. You can create your own keywords. Be sure that the keyword matches the value for the **-as** name flag you used when starting the proxy in a startup script

Table 2-1 Common Keywords and Associated Applications

Keyword	Application
ahttp-gw	Authenticating HTTP proxy (using the HTTP proxy)
aol-gw	America Online proxy (using the plug proxy with -as)
authenIP	IP screening configuration applications
authsrv	Authentication server
ck-gw	Circuit proxy
cserve-gw	CompuServe proxy (using the plug proxy with -as)
finger	Proxy for *finger*.
ftp-gw	FTP proxy
gopher-gw	Gopher proxy (using the HTTP proxy with -as)

Table 2-1 (continued) Common Keywords and Associated Applications

Keyword	Application
gui	Gauntlet Firewall Manager
http-gw	HTTP proxy
info-gw	Web and Gopher server (Info proxy)
lnotes-gw	Lotus Notes proxy (using the plug proxy with -as)
login-sh	Login shell
lp-gw	Line printer proxy
mbase-gw	MediaBase proxy
mmp	Multimedia proxy
mssql-gw	Microsoft SQL proxy
netacl-fingerd	Network access control proxy running finger service
netacl-ftpd	Network access control proxy running FTP service
netacl-rlogind	Network access control proxy running rlogin service
netacl-telnetd	Network access control proxy running telnet service
netconfig	IP screening configuration applications
NetShow	NetShow proxy (using the mmp proxy)
nntp-gw	NNTP news proxy (using the plug proxy with -as)
pcxdpp	PC Extender DPP daemon
plug-gw	Plug proxy
policy-name	Policy
pop3-gw	POP3 mail proxy
radm	Remote administration scripts
RealAudio	RealAudio/RealVideo proxy (using the mmp proxy)
rlogin-gw	Rlogin proxy
rsh-gw	Remote shell proxy

Table 2-1 (continued) Common Keywords and Associated Applications

Keyword	Application
smap	SMTP mail client
smapd	SMTP mail server
snmpd	SNMP network management agent
snmp-gw	SNMP network management proxy
ssl-gw	SSL proxy (using the plug proxy with -as)
strmwrks-gw	Streamworks proxy
syb-gw	Sybase proxy
tn-gw	TELNET proxy
VDOLive	VDOLive proxy (using the mmp proxy)
whois	whois proxy (using the plug proxy with -as)
x-gw	X11 proxy

Attributes in Netperm Tables

Attributes vary by proxy and application, though some attributes are common to multiple applications. Consult the reference information in Chapter 4, “Attribute Reference,” for more information on applicable attributes and values.

Chapter 3

Policies and Services

This chapter tells you how to create new policies, add or deny proxy services, deny services by network or host, and control services by user, group, or time. The chapter has the following sections:

- "Creating New Policies" on page 11
- "Adding Proxy Services" on page 13
- "Denying Proxy Services" on page 14
- "Denying Services by Network or Host" on page 14
- "Controlling Services by User, Group, or Time" on page 16

Creating New Policies

You can create additional policies to fit your security requirements for different groups of inside hosts and networks. Remember that all policies are based on the source address of the request. Creating a new policy involves modifying the netperm table.

How to Create a New Policy

To create a new policy:

1. Add a line indicating:
   - Source networks that use the policy
   - Name of the policy
2. Add rules indicating which proxies this policy allows.
3. Add rules indicating permitted destinations, authentication, and logging.
4. Place the policy lines above or below the section generated by the Gauntlet Firewall Manager, as appropriate (see "Precedence in Netperm Tables" on page 6).

Example for Creating a New Policy

Suppose, for example, that the generic policy for Yoyodyne uses the default Gauntlet trusted policy. The security policy for Yoyodyne calls for restricting a particular group of systems (and set of addresses) to TELNET and rlogin to a particular set of outside networks.

To implement this policy, you can create a more restrictive policy:

```
1     #define inside hosts who will use the policy
2     *: permit-hosts 204.255.154.0:255.255.255.128 -policy restrictive
3     #define the policy
4     policy-restrictive: permit-proxy netacl-telnetd tn-gw
5     policy-restrictive: permit-proxy netacl-rlogind rlogin-gw
6     policy-restrictive: permit-destination 192.33.112.*
7     policy-restrictive: authenticate *
8     policy-restrictive: authserver 127.0.0.1
```

- Line 2 indicates that all proxies and applications (*) should use the restrictive policy for requests from the designated subnet. If you specify the policy for only the TELNET (tn-gw) and rlogin (rlogin-gw) proxies instead of for all (*), all other proxies (such as the HTTP and FTP proxies) skip this policy and use another policy.
- Lines 4 and 5 indicate that this policy permits the TELNET and rlogin proxies. All other proxies with requests from hosts within 204.255.154.0:255.255.255.128 deny the request after parsing these lines.
- Line 6 indicates that these proxies can send requests to the set of destinations: 192.33.112.*. The TELNET and rlogin proxies deny requests to any other destinations after parsing this line.
- Lines 7 and 8 indicate that users on these networks must authenticate with the authentication server on the firewall.

You must put this policy above the trusted policy so the proxies will use these rules rather than the more permissive trusted policy. You may also want to create a matching restrictive untrusted policy to restrict access from outside networks to this internal subnet.

Note that this type of policy may not prevent users on this inside network from reading news and sending e-mail. The recommended setup for the Gauntlet firewall calls for central mail and news servers on the inside networks. The news readers and mail agents on the restricted subnet communicate directly with the news and mail servers. These servers, which are not on the restricted subnet, communicate directly with the firewall.

If, however, you are running mail and news servers on the firewall, this more restrictive policy does deny e-mail and news activities from the restricted subnet.

Adding Proxy Services

You can add proxy services at any point as your security policies change. This section addresses the changes you must make to the netperm table to use the proxy. See the *Gauntlet for IRIX Administrator's Guide* for information on other configuration requirements for the various proxies.

To add a proxy service:

1. Add the name of the proxy to the permit-proxy line of the appropriate policy.
2. Add a section for proxy-specific rules above the policy sections. These rules can include items such as userid, groupid, time-out, and denial messages. Consult the reference information for the proxy for information on proxy options.

For example, suppose that Yoyodyne wants to add support for Quote of the Day (qotd) service for users on its inside networks. This involves using the proxy. First, add a line to the trusted policy:

```
99    policy-trusted: permit-proxy qotd-gw
```

Next, create a section above the policies in which you define the communications rules for the Quote of the Day connection:

```
95    # QotD (through plug proxy) rules
96    # ---------------------------------------
97    qotd-gw: port qotd * -plug-to qotd.bigu.edu -port qotd
```

Denying Proxy Services

You can remove proxy services as your security policies change. You can use the Proxy Configuration options in the Gauntlet Manager graphical user interface, or you can modify the netperm table.

To remove a proxy service, remove or comment out the permit-proxy line in the appropriate policy.

For example, assume Yoyodyne no longer wishes to allow users to rlogin from outside networks. The administrator modifies the untrusted policy:

```
44    #policy-untrusted: permit-proxy rlogin-gw
```

Denying Services by Network or Host

You can deny services to and from specific networks and hosts. You can do this for all the proxies through a policy, or for individual proxies.

When you deny service, you can specify by IP address or by host. If you specify by IP address, proxies deny access based on that IP address. Be sure that you explicitly deny all IP addresses a system or site may have.

Because, in most cases, a proxy sees an IP address for only a given connection request, there are additional considerations when specifying hostnames in permit or deny rules. The firewall must perform additional processing steps to convert the address that is in the packet and the hostname that is in the configuration rule to the same format so that it can compare the values.

If you deny by hostname, the proxy must use DNS to map the source or destination address (in the packet) into a hostname. If the proxy cannot perform this mapping, it considers the address to be unknown.

Denying Access From a Host or Network

You can deny access from a particular host or network on a per-proxy basis or on a general basis.

Denying Access by Proxy

To deny access by proxy, add a deny-hosts line to the specific proxy.

For example, Yoyodyne does not want anyone on any system at Big University to have TELNET access to Yoyodyne:

```
50    tn-gw: deny-hosts *.bigu.edu
```

Later, Yoyodyne determines they need to deny access only from the dial-in systems at Big University:

```
50    tn-gw: deny-hosts dial*.bigu.edu
```

Denying Access From a Host or Network

You can also deny access from a particular host or network for all proxies and applications.

To deny access for all applications, add a deny-hosts line above the untrusted policies. Use a wildcard as the keyword to indicate that the rule applies to all policies.

You must include this rule above the policy rules. The policies are based on permitted hosts. Including the deny-hosts rule in a policy has no effect because the application is using the permit-hosts rule that defines the policy.

Note that the SMAP proxies do not use the policy rules, so you still receive mail from the denied host or network.

For example, Yoyodyne does not want anyone or any service at Big University to communicate with Yoyodyne:

```
103   *: deny-hosts *.bigu.edu
...
140   *: permit-hosts * -policy outside
```

Denying Access to a Host, Network, or Proxy

You can deny access to a particular host or network on a proxy or general basis.

Denying Access by Proxy

To deny access by proxy, add a deny-destination line to the specific proxy.

For example, Yoyodyne does not want anyone on the inside networks to transfer files using FTP from any hosts at Big University:

```
55    ftp-gw: deny-destination *.bigu.edu
```

Denying General Access to a Host or Network

You can also deny access to a particular host or network for all proxies and applications.

To deny access for all applications, add a deny-destination line to the appropriate policy.

For example, Yoyodyne does not want anyone on the inside network to communicate with Big University:

```
108   policy-trusted: deny-destination *.bigu.edu
```

Note that the SMAP proxies do not use the policy rules, so you can still send mail to the denied host or network.

Controlling Services by User, Group, or Time

You can control access to the following proxies on a per user, per group, or time of day basis:

ck-gw	Circuit proxy
ftp-gw	FTP proxy
rlogin-gw	Rlogin proxy
rsh-gw	Rsh proxy
tn-gw	TELNET proxy

Controlling Services by User or Group

You can permit or deny access to certain proxies by user or group as follows:

1. Add the *operations* attribute to your authsrv configuration to specify who can perform the operation and what services they can access.
2. Add the *authenticate* attribute to the appropriate policy or proxy to require users to authenticate before using the service.
3. Add the *extended-permissions* attribute to the appropriate policy or proxy to indicate that the authentication server should check information specified by the operations keyword.

For example, Yoyodyne wants to permit only members of the group Developer to use the rlogin proxy when accessing outside hosts:

```
55    authsrv: permit-operation group Developer rlogin-gw *
....
100   rlogin-gw: authenticate *
101   rlogin-gw: extended-permissions *
```

These commands prevent any other users who are not members of group Developer (in the Gauntlet authentication database) from using the rlogin proxy.

Controlling Services by Operation

You can permit or deny access to certain proxies by time of day.

To control access by time of day:

1. Add the *operations* attribute to your authsrv configuration to specify who can perform what operations, and what services they can access, and when.
2. Add the *authenticate* attribute to the appropriate policy or proxy to require users to authenticate before using the service.
3. Add the *extended-permissions* attribute to the appropriate policy or proxy to indicate that the authentication server should check information specified by the operations keyword.

Suppose, for example, that Yoyodyne wants to deny TELNET between 5:00 p.m. and 11:00 p.m.:

```
55    authsrv: deny-operation user * tn-gw * * time 17:00 23:00
56    authsrv: permit-operation user * tn-gw * *
...
100   tn-gw: authenticate *
101   tn-gw: extended-permissions *
```

Line 55 denies TELNET access between 5:00 p.m. and 11:00 p.m.

Line 56 permits TELNET access. You must include this rule because you must explicitly permit operations when you specify extended permissions.

The deny rule must appear before the permit rule because the proxies use the first matching rule. If you specify the permit rule before the deny rule, the authentication server would never read the deny rule, because the permit rule matches all TELNET operations.

Chapter 4

Attribute Reference

This chapter lists and describes all netperm table attributes.

The chart for each attribute indicates which proxies, applications, or policies can use that attribute. For example, a bullet (•) next to tn-gw means you can use this attribute for the TELNET proxy.

A bullet next to policy indicates that you can use this attribute in a policy definition. All proxies that use this policy use this attribute.

You can always use any attribute after the wildcard (*) keyword. *All* proxies read this rule.

Note: The **http-gw** keyword in the tables on the following pages indicates the HTTP proxy regardless of whether the authentication option of HTTP is enabled or disabled. Rules marked with the **ahttp-gw** keyword are active *only* when the authentication option is enabled.

See "Netperm Table Format" on page 6 for more information on how attributes are used.

accept-count

Specifies how many processes the proxy forks to listen for connections on a port.

ahttp-gw	• gopher-gw	• mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	• info-gw	NetShow	smap	VDOLive
• authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	snmp-gw	policy-*policy*
• finger	• lp-gw	• pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	• ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

accept-count *processes*

processes Number of processes the proxy should fork.

Example

```
http-gw: accept-count 50
```

The HTTP proxy forks 50 processes to listen for connections.

admin-user

Specifies the name of the administrative user for the firewall, which the Gauntlet Firewall Manager uses to authenticate before making changes to the firewall's configuration.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	• gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

admin-user *user*

user Name of the administrative user for the firewall. This account must exist in the authentication database.

Example

```
gui: admin-user fwadmin
```

The Gauntlet Firewall Manager prompts for authentication information from fwadmin before making changes to the firewall's configuration.

Gauntlet Firewall Manager

Environment > Firewall Access tab > UserName

agent

Specifies the name of a network management agent that the SNMP proxy can contact.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	• snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-agent *host* [get | !get] [set | !set] [trap | !trap]

permit	Agents to which the proxy can send information.
deny	Agents to which the proxy cannot send information.
host	Name of a network management agent that the SNMP proxy can contact. Specify by IP address or hostname.
get	The proxy allows the network manager to access information on this agent.
!get	The proxy does not allow the network manager to access information on this agent.
set	The proxy allows the network manager to set information on this agent.
!set	The proxy does not allow the network manager to set information on this agent.

trap	The proxy allows this agent to send traps to the network manager.
!trap	The proxy does not allow this agent to send traps to the network manager.

Example

```
snmp-gw: permit-agent 204.255.154.3 trap
```

The SNMP proxy allows the agent on the system 204.255.154.3 to send traps to the network manager.

Gauntlet Firewall Manager

Services > SNMP tab > Configure > HostName or IP Address

anon-user

Specifies the string that the HTTP proxy provides to anonymous FTP servers when prompted for a user name as a password. If you do not use this attribute, the proxy sends the string `httpgw@`.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

anon-user *password*

password String that the HTTP proxy provides to anonymous FTP servers when prompted for a user name as a password. Any printable ASCII characters, except space or tab, are valid.

Example

```
http-gw: anon-user firewall-user@yoyodyne.com
```

The HTTP proxy should use the name firewall-user@yoyodyne.com when prompted for a user name as a password by an anonymous FTP server.

authenticate (all but pcxdpp)

Specifies whether or not users must authenticate when accessing these proxies. Proxies that do not support authentication ignore this setting. This is equivalent to the **–auth** and **–authall** options in previous versions.

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	• pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

authenticate *

*Provided for future extensibility.

Example

```
policy-untrusted: authenticate *
```

All requests from hosts on the outside network must authenticate.

Gauntlet Firewall Manager

Firewall Rules > Service Groups tab > AuthServer

authenticate (pcxdpp only)

Specifies whether the DPP daemon considers links between the firewall and the PC to be trusted or untrusted. If you use the authenticate attribute, the DPP daemon considers the link to be private. If you do not use the authenticate attribute, the DPP daemon considers the link to be trusted.

This attribute is optional. If you do not specify it, the DPP daemon uses the authenticate settings for the trusted or untrusted policy, as appropriate.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	• pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

authenticate *

*Provided for future extensibility.

Example

```
pcxdpp: authenticate
```

The DPP daemon considers the link between the firewall and PC Extender to be private.

authserver

Specifies the host that is running the authentication server that the proxies use for authenticating users.

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	• login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	• pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

authserver *host* [*port*]

host Host running the authentication server. Specify IP address or hostname.

port Port on the host that the proxies use for communicating with the authentication server.

Example

```
policy-untrusted: authserver 127.0.0.1 7777
```

Proxies must use the authentication server on the firewall itself using port 7777.

Gauntlet Firewall Manager

Firewall Rules > Service Groups tab > AuthServer and Port

authtype

Obsolete. Use the authserver attribute (see “authserver” on page 27).

backend

Name of the executable to which the authenticating HTTP proxy passes requests after handling the authentication. The executable handles FTP, Gopher, and other protocols.

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

backend *executable*

executable Name of the executable to which the authenticating HTTP proxy passes requests after handling the authentication.

Example

```
ahttp-gw: backend /usr/etc/http-gw
```

The authenticating HTTP proxy passes processing to */usr/etc/http-gw*.

badadmin

Specifies the user name to which the *smapd* server forwards mail that it cannot deliver.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

badadmin *user*

user Name of a user or alias.

Example

```
smapd: badadmin firewalladmin
```

Send mail to the firewalladmin alias.

Gauntlet Firewall Manager

Environment > Mail tab > SMAP > Notify for undeliverable mail

baddir

Specifies the directory in which the *smapd* server places any spooled mail that it cannot deliver normally.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

baddir *directory*

directory Name of a directory on the same device as the spool directory. Do not include a trailing slash (/) character. Ensure that this directory exists and has the same owner and permission as the directory that smap normally uses.

Example

```
smapd: baddir /var/spool/smap/badmail
```

Places the undelivered mail in the */var/spool/smap/badmail* directory.

Gauntlet Firewall Manager

Environment > Mail tab > SMAP > Place undeliverable mail here

badsleep

Specifies for how long the authentication server disallows logins from a user who has attempted (and failed) to log in five times in a row.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

badsleep *seconds*

seconds Number of seconds the authentication server sleeps before allowing login attempts from a user who has attempted (and failed) to log in five times in a row. If this attribute is set to 0, the authentication server allows an unlimited number of unsuccessful login attempts. If this attribute is not set, the authentication server disables the account after the user attempts (and fails) to log in five times in a row.

Example

```
authsrv: badsleep 1200
```

The authentication server sleeps for 20 minutes (1200 seconds) after five unsuccessful login attempts.

bind-address

Specifies the IP address to which a proxy is bound. Binding a proxy to a particular address allows you to offer that service only for requests to that address. This attribute is useful when you have assigned multiple IP addresses to one of your network interface cards, and want to allow only a particular type of traffic for one of those addresses.

You can bind different proxies to different addresses, but all of these proxies can use the same port. This configuration is useful when you need to offer multiple services on the same port, but with different addresses. When using bind-address, you must also run a new version of the proxy, create a startup script for the proxy, create a policy that uses the new proxy.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	• info-gw	NetShow	smap	VDOLive
• authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	• login-sh	• plug-gw	snmp-gw	policy-*policy*
• finger	• lp-gw	• pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	• ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

bind-address *address*

address IP address to which you want to bind a proxy.

Example

```
aol-gw: bind-address 204.255.154.1
```

Bind the AOL proxy to the IP address 204.255.154.1.

bind-inside

Specifies the inside interface and address of the trusted network inside the firewall. Used to create the packet screening rule that denies packets on the outside interfaces with trusted network addresses to prevent IP spoofing.

ahttp-gw	gopher-gw	• mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	• syb-gw
alerts	http-gw	• netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

bind-inside -if *insideinterface* -addr *insidenetwork*

insideinterface Interface name of the inside interface of the firewall for example, ec0. Valid values vary by type of physical connection.

insidenetwork IP address and subnet mask of a trusted network inside the firewall. The * wildcard is valid.

Example

```
netconfig: bind-inside -if ec0 -addr 10.0.1.0:255.255.255.0
```

Inside interface of firewall is ec0 and network inside the firewall uses 10.0.1.* addresses.

block

Specifies that the FTP proxy does not allow file transfers of designated types.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

block { input | output }

input	The FTP proxy does not allow file transfers from server to client.
output	The FTP proxy does not allow file transfers from client to server.

Example

```
ftp-gw: block output
```

The FTP proxy prevents file transfers from client to server.

buffer-size

Specifies the size of the internal buffer that the proxy uses for transferring data. If you do not use this attribute, the proxy uses a buffer of 16,384 bytes.

If you use this attribute and specify an invalid value (for example, a negative number), the proxy uses a buffer of 8,192 bytes.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	snmp-gw	policy-*policy*
• finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	• ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

buffer-size *buffer*

buffer Size of the internal buffer that the proxy uses for transferring data.

Example

```
ssl-gw: buffer-size 32768
```

The SSL proxy uses an internal buffer size of 32,768 bytes.

check-server-ip

Specifies whether or not the proxy checks the IP address of the server sending the packets against the IP address in the clients request. By default, the proxy compares the IP address in the client request to the IP address in the incoming packets. If the IP addresses do not match, the proxy drops the packet.

Some multimedia sites use multiple servers to service requests. By default, the proxy drops packets. If your users need to access these types of sites, use this attribute to turn off IP checking on incoming packets.

ahttp-gw	gopher-gw	mssql-gw	• RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	• NetShow	smap	• VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	• mbase-gw	
ftp-gw	• mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

check-server-ip { 0 | 1 }

0	Proxies check the IP address of the incoming packets against the IP address in the client request. If the IP addresses do not match, the proxy drops the packet.
1	Proxies do not check the IP address of the incoming packets against the IP address in the client request.

Example

```
mmp-gw: check-server-ip 1
```

The multimedia proxy does not check the IP address of incoming packets against the IP address in the client request.

child-limit

Specifies the maximum number of child processes that each daemon allows to run at the same time.

ahttp-gw	• gopher-gw	• mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	• netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	• info-gw	NetShow	smap	VDOLive
• authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	• snmp-gw	• policy-*policy*
• finger	• lp-gw	• pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	• ssl-gw	

Syntax

child-limit *processes*

processes Maximum number of child processes that each daemon allows to run at a given time. If this attribute is set to 0 or is not set, the daemon allows an unlimited number of child processes to run at the same time.

Example

```
tn-gw: child-limit 10
```

The TELNET proxy allows only ten child processes to run at the same time.

Gauntlet Firewall Manager

Services > Service tab > ChildLimit

circuitexec

Specifies the location of the program that the circuit proxy runs once it allows a connection from the client program.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

circuitexec *programs*

programs Location and name of the program that the circuit proxy runs once it allows a connection from the client program.

Example

```
ck-gw: circuitexec /usr/local/etc/circuit
```

The circuit proxy is in */usr/local/etc*.

Gauntlet Firewall Manager

You cannot set this attribute through the Gauntlet Firewall Manager.

circuitsperuser

Specifies the maximum number of client/server connections that can be active in one user session.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

circuitsperuser *circuits*

circuits Maximum number of client/server connections that can be active in one user session.

Example

```
ck-gw: circuitsperuser 12
```

A user can have 12 active sessions.

Gauntlet Firewall Manager

Services > Circuit tab > Add or Modify > # Circuits allowed per user

circuit-timeout

Specifies the amount of time the client/server connection is idle (no network activity) before disconnecting. Overridden by the **-timeout** option of the server attribute for a particular server. See “server” on page 120

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

circuit-timeout *minutes*

minutes Number of minutes without client/server activity before disconnecting.

Example

```
ck-gw: circuit-timeout 15
```

The client/server activity can be idle for 15 minutes before disconnecting.

Gauntlet Firewall Manager

Services > Circuit tab > Add or Modify > Circuit Timeout

client

Specifies the *lp* commands that the firewall denies or logs from clients to remote server queues.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	• lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

client *clients* -printer *serverqueue* [{-deny | -log} [{ *lpcommands* } | all]]

clients	Specifies single hosts, entire networks, or subnets. Specify by IP address or hostname. The wildcard * is valid.
serverqueue	Name of the printer queue on the remote server to which this rule applies.
deny	Commands that clients cannot execute. The default allows users to issue all *lp* commands.
log	Extended logging applies. Extended logging includes the number of bytes transferred from client to server and time duration. Extended logging does not include data transfer from server to client, as this consists mostly of acknowledgments to client's command.
lpcommands	*lp* commands that the clients can issue when sending jobs through the proxy. The space between the "{" and "}" and the list entries is required. Valid keywords, which correspond to the first level *lp* protocol commands, are: • **restart** • **print** • **status_sh** • **status_ln** • **remove**
all	The deny or log attribute applies to all *lp* commands.

Example

```
lp-gw: client 10.0.1.* -printer lp_sales -log {restart remove}
```

The proxy logs the restart and remove commands when any clients on the inside network (10.0.1.*) print to the remote printer queue lp_sales (on the remote server).

Gauntlet Firewall Manager

Services > LP tab > Add or Modify > Client Queue

connect-timeout

Specifies the amount of time the user has to start the client application before the proxy stops listening at the service port. This attribute also controls the amount of time the user has to respond to the query asking them to allow the connection.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

connect-timeout *minutes*

minutes Number of minutes the proxy waits at the service port for a client application connection before it disconnects.

Example

```
ck-gw: connect-timeout 3
```

The user has three minutes to start the client application before the proxy stops listening.

Gauntlet Firewall Manager

Services > Circuit tab > Add or Modify > Connect Timeout

content-failunsafe

Specifies whether or not the content-scanning enabled proxies allow data transfers when content scanning is enabled but not working (for example, the server is unreachable). The proxies normally exit when a transfer is attempted while content scanning is broken so that unscanned data cannot enter your protected network.

If content-failunsafe is not used (it is off by default), the content-enabled proxies do not allow data transfers when content scanning is enabled but not working. This attribute has no effect when content scanning is not enabled.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

content-failunsafe {on | off}

Example

```
ftp-gw: content-failunsafe on
```

The FTP proxy (when content scanning is enabled) allows data transfers even when content scanning is not working.

content-ftpcheck

Specifies the types of transfers for which the FTP proxy should scan the contents of the files. Use this attribute as part of a policy, rather than for the proxy itself.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

content-ftpcheck *types*

types Types of transfers for which the FTP proxy scans the contents. Valid keywords are:

- **retr**—Scan files that are being transferred from server to client.
- **stor**—Scan files that are being transferred from client to server.

Example

```
policy-untrusted: content-ftpcheck retr stor
```

When the FTP proxy is used as part of the untrusted policy, it scans all files being transferred.

Gauntlet Firewall Manager

Services > FTP tab > Add or Modify > Scan FTP Puts or Scan FTP Gets

contentscan-msg

Specifies the name of the file that the proxy displays as a welcome banner upon successful connection to the proxy when content scanning is enabled. If this attribute is not used, the proxy generates a default welcome message.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

contentscan-msg *file*

file Name of the file that the proxy displays as a welcome banner upon successful connection to the proxy when content scanning is enabled.

Example

```
ftp-gw: contentscan-msg /usr/local/etc/ftp-contentscan-msg.txt
```

The FTP proxy displays the contents of the file */usr/local/etc/ftp-contentscan-msg.txt* upon successful connection when content scanning is enabled.

Gauntlet Firewall Manager

Services > FTP tab > Add or Modify > CVP Welcome Msg

cvp-handling

Specifies the type of handling to use when the proxy receives a file or message that failed the content scan.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

cvp-handling { reject | repair }

reject — The proxy discards the failed file or message.

repair — The proxy attempts to repair the message. If the repair is successful, the proxy delivers the file or message.

Example

```
http-gw: cvp-handling reject
```

The HTTP proxy discards all files that fail the content scan.

Gauntlet Firewall Manager

Services > FTP or HTTP tab > Add or Modify > Infected File Handling

Environment > Mail > Infected File Handling

cvp-server

Specifies the server that the proxy uses for content scanning services.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

cvp-server *host port*

host Host running the content scanning server. Specify by IP address or hostname. Wildcards are not valid.

port Port on the host on which the content scanning server is running.

Example

```
ftp-gw: cvp-server 10.0.1.57 18181
```

The FTP proxy uses a content scanner on the system `10.0.1.57` using port 18181.

Gauntlet Firewall Manager

Services > FTP or HTTP tab > Add or Modify > CVP HostName and CVP Port

Environment > Mail > CVP HostName and CVP Port

cyber_masks

Lets you specify what Cyber Patrol categories are blocked for work time hours and leisure time hours. Categories not blocked are allowed.

This attribute has no effect unless Cyber Patrol is active. Refer to the *Gauntlet Firewall Administrator's Guide* for descriptions of each category listed under "Syntax."

Use this attribute as part of a policy, rather than for the proxy itself.

See also the attributes "feature" on page 64, "url" on page 132 and "work_time" on page 142.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

policy-http-gw_Trusted: cyber_masks *work_mask leisure_mask*

work_mask The bitmasks for Cyber Patrol categories that are denied during work time hours. The categories are:

- Violence/Profanity—0x0001
- Partial Nudity—0x0002
- Full Nudity—0x0004
- Sexual Acts/Text—0x0008

- Gross Depictions/Text—0x0010
- Intolerance—0x0020
- Satanic/Cult—0x0040
- Drugs/Drug Culture—0x0080
- Militant/Extremist—0x0100
- Sex Education—0x0200
- Questionable/Illegal & Gambling—0x0400
- Alcohol/Tobacco—0x0800
- Sports/Leisure—0x1000
- Not Yet Used #1—0x2000 *
- Not Yet Used #2—0x4000 *
- Search Engines—0x8000

  * Reserved for future categories. Setting these bits has no effect.

To determine the bitmask for a group of categories, use a hexadecimal calculator.To determine the bitmask for Violence, Partial Nudity, Full Nudity and Sexual Text, for example, enter **`0001`** (for Violence), click *OR*, then enter **`0002`** (for Partial Nudity), click *OR* again, then **`0004`** (for Full Nudity), click *OR*, then enter **`0008`** (for Sexual Acts/Text), and click *OR* a final time. The result, `F`, is the bitmask for these three categories. You can perform the same procedure for any combination of categories.

leisure_mask The bitmasks for Cyber Patrol categories that are denied during leisure time hours. The categories are the same as for *work_mask*.

Example

```
policy-http-gw_Trusted: cyber_masks 1FFF FFF
```

All Cyber Patrol categories except Search Engines are denied during work time hours, while all categories except Search Engines and Sports/Leisure are denied during leisure time hours.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Cyber Patrol

data-port

Specifies that the FTP proxy requires FTP data connections to use port 20, the default port specified in the RFC for FTP. By default, the FTP proxy uses a random, nonprivileged port for the data connection. Some FTP software packages and routers require that the data connection use port 20.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

data-port *port*

port Port name or number on which the FTP proxy listens for data connections.

Example

```
ftp-gw: data-port 20
```

FTP proxy requires data connections on port 20.

database (authsrv only)

Specifies the pathname of the database that the authentication server uses. This attribute is mandatory, unless you compile the authentication server with a specific database path.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

database *path*

path Path of the database that the authentication server uses.

Example

```
authsrv: database /usr/local/etc/fw-authdb
```

The authentication server uses the authentication database in */usr/local/etc/fw-authdb*.

database (pcxdpp only)

Specifies the pathname of the database that the authentication server uses to check administrative keys for PC Extender to firewall links.

This attribute is required.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	• pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

database *path*

path Pathname of the database that the authentication server uses to check administrative keys.

Example

```
pcxdpp: database /usr/local/etc/mgmt/dpp-authdb
```

The authentication server uses the database */usr/local/etc/mgmt/dpp-authdb*.

database (pop3-gw only)

Specifies the pathname of the database that the authentication server uses to authenticate POP3 users.

This attribute is required if the authentication option of POP3 is enabled.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	• pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

database *path*

path Pathname of the database that the authentication server uses to authenticate POP3 users.

Example

```
pop3-gw: database /usr/local/etc/mgmt/pop3-authdb
```

The authentication server uses the database */usr/local/etc/mgmt/pop3-authdb*.

Gauntlet Firewall Manager

Environment > Mail > Pop3 > AuthServer Database

denial-msg

Specifies the file that the proxy displays when it denies access because a user does not have permission to use the proxy.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

denial-msg *file*

file Name of the file the proxy displays when it denies access because a user does not have permission to use the proxy. If no file is specified, the proxy generates a default message.

Example

```
ftp-gw: denial-msg /usr/local/etc/ftp-deny.txt
```

Displays the file */usr/local/etc/ftp-deny.txt* when the FTP proxy denies access to a user.

Gauntlet Firewall Manager

Services > Service tab > Add or Modify > Deny Use Message

denydest-msg

Specifies the file the proxy displays when it denies access because a user is trying to access a destination that he or she is not permitted to access.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

denydest-msg *file*

file Name of the file the proxy displays when it denies access to a user who tries to access a disallowed destination. If no file is specified, the proxy generates a default message.

Example

```
tn-gw: denydest-msg /usr/local/etc/tn-denydest.txt
```

Displays the file */usr/local/etc/tn-denydest.txt* when the TELNET proxy denies access to a user.

Gauntlet Firewall Manager

Services > Service tab > Add or Modify > Deny Destination

deny-spam

Adds unwanted domain names and email addresses to your anti-spam database. Keep in mind that specifying a particular email address is not foolproof. A remote mailer can lie about its address but not about its domain.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

deny-spam *address*

address Domain name or email address for which you want to deny all messages.

Example

```
smap: deny-spam spammer@spam.com
```

Blocks all messages from spammer@spam.com

destination

Specifies destination hosts and network permissions.

• ahttp-gw	• gopher-gw	• mssql-gw	• RealAudio	• strmwrks-gw
• aol-gw	• gui	• netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	• info-gw	• NetShow	smap	• VDOLive
authsrv	• ldap-gw	• nntp-gw	smapd	• whois
• ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	• snmp-gw	• policy-*policy*
• finger	• lp-gw	• pop3-gw	• mbase-gw	
• ftp-gw	• mmp	radm	• ssl-gw	

Syntax

{permit | deny}-destination *destination-list*

permit *destination-list*
: Hosts to which the proxies and applications can send requests.

deny *destination-list*
: Hosts to which the proxies and applications cannot send requests.

destination-list
: Single hosts, entire networks, or subnets. Specify by IP address or hostname. The wildcard * is valid. Use the word unknown to match hosts that do not have DNS entries or whose forward and reverse lookups do not match. Specify multiple destinations using braces {} and separating the items with spaces. If no *destination-list* is specified, no destinations are valid.

Example

```
policy-restrictive: permit-destination 192.3.4.*
```

Permits applications to send requests to hosts on the 192.3.4 network

Gauntlet Firewall Manager

Firewall Rules > Service Groups tab > Destinations

Services > Service tab > Destinations

Services > Service tab > Add or Modify > Destinations

directory (gui, info-gw, smap and smapd only)

Specifies the directory that the proxy uses as the root of its database. For the smap and smapd proxies, specifies the directory where messages should be stored.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	• gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	• info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

directory *directory*

path Specifies the directory that the proxy uses as the root of its database.

Example

```
smap, smapd: directory /var/spool/smap
```

The *smap* and *smapd* proxies use the directory */var/spool/smap* to store messages.

Gauntlet Firewall Manager

Environment > Mail > SMAP > Spool Location;

Services > Info tab > Database

directory (all others)

Specifies that the proxy should move into a new root directory, known as a "locked room" before providing service. This attribute is equivalent to the **-chroot** option in previous versions.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	• strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	• lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

directory */usr/local/etc/mgmt/proxies_root*

No other value is valid for this attribute.

Example

```
http-gw: directory /usr/local/etc/mgmt/proxies_root
```

The http-gw proxy runs in a locked room environment.

Gauntlet Firewall Manager

Services > Service tab > Locked Room

display

Specifies the destination display on which applications display.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	• x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	sql-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

display *host:displaynumber.screennumber*

host	Name of the system to which the display is physically connected.
displaynumber	Number of the display on the system.
screennumber	Number of the screen for the display.

Example

```
x-gw: display redwood :10.0
```

The X gateway displays all X applications on the display attached to the redwood system.

exec

Specifies a program that the proxy invokes to handle a service. This attribute is equivalent to the **-exec** option in previous versions.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	• netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

exec *program* [*options*]

program Name of the program to invoke.

options Command line options for the program.

Example

```
netacl-fingerd: exec /bin/cat /usr/local/etc/finger.txt
```

The *netacl* daemon invokes the *cat* program to display the file */usr/local/etc/finger.txt* for *finger* requests.

extended-permissions

Specifies whether the proxies check for extended permissions for users as they authenticate. Checking for extended permissions tells the authentication server to obey the attribute's keywords when it reads the netperm-table. This attribute is equivalent to the **-extend** and **-extnd** options in previous versions. When you turn on extended permissions, the proxies that use extended permissions deny all operations. You must then explicitly permit the proxies to allow activities by creating rules using the operations attribute. Use care when specifying extended permissions for policies.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

extended-permissions *

Example

```
ftp-gw: extended-permissions *
```

FTP proxy checks for extended permissions when authenticating users.

Gauntlet Firewall Manager

Firewall Rules > Users tab > Restrictions; Services > Service tab > Add or Modify > Restrictions

feature

Specifies particular features explicitly permitted or denied. Denying a feature causes the HTTP proxy to remove the related tags from within the HTML code. Lets you control general features rather than specific portions of the HTTP protocol.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax 1

http-gw: {permit | deny}-feature *features*

features Lists particular HTTP features.

Valid features are:

- activeX (deny removes <EMBED> and <OBJECT> tags)
- frames
- html2
- cyberpatrol (permit activates support for Cyber Patrol software)
- java (deny removes <APPLET> tags)
- script (deny removes <SCRIPT> tags>)
- kanji (permit allows Kanji characters as described in RFC 1468)
- legacy-kanji (permit allows Kanji characters as implemented in Gauntlet 3.2)
- multipart-form (blocks a file upload bug in Netscape Navigator)

Example

```
http-gw: deny-feature java javascript
```

The HTTP proxy removes Java or JavaScript tags from within any HTML accessed through the proxy.

```
policy-http-gw_Trusted: permit-feature cyberpatrol
```

Cyber Patrol is enabled at the policy level.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Deny Special Features

You cannot set portions of this attribute through the Gauntlet Firewall Manager.

Syntax 2

Specifies features in which the HTTP proxy restricts HTML to comply with that feature type.

http-gw: feature *features*

features	Lists particular HTTP features. Valid features are: frames, html2, java, script

Example

```
http-gw: feature html2
```

The HTTP proxy removes from any HTML that it accesses all HTML that does not meet the HTML2 standards.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Deny Special Features

You cannot set portions of this attribute through the Gauntlet Firewall Manager.

force_source_address

Specifies that the plug proxy uses the IP address of the originating host as the source address of the packet when sending a request to the destination host.If this attribute is not specified, the firewall uses its own IP address as the source address of the packet, causing all packets to look as if they originated on the firewall.You must use officially registered, routable addresses on your trusted networks to use this attribute.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	• rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	• ssl-gw	

Syntax

force_source_address { on | off }

Example

```
aol-gw: force_source_address on
```

The plug proxy for America Online uses the IP address of the originating host as the source address of the packet when sending the packet on to the destination host.

Gauntlet Firewall Manager

Services > Plug tab > Add or Modify > Source Address

You cannot set this attribute through the Gauntlet Firewall Manager for some proxies.

forward

Specifies the name of a host to which the HTTP proxy forwards requests for which it can find no destination information.

The HTTP proxy uses this information as a last resort, when it cannot find any other information in the request. This may happen when transparency is not enabled.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

forward *pattern* -protocol *protocol* -tohost *host:port*

pattern Pattern in the URL for which the HTTP proxy uses this rule. Quotation marks are not required.

-protocol *protocol*
Protocol that the HTTP proxy uses when communicating with the remote host. Valid values are FTP, Gopher, and HTTP

-tohost *host:port*
Host and port to which the HTTP proxy forwards requests and the port on which it connects. Use IP addresses or hostnames. Specify ports by port number.

Example

```
http-gw: forward /pub* -protocol ftp -tohost ftp.bigu.edu
```

The HTTP proxy forwards all requests with a URL starting with the string "/pub" to the host ftp.bigu.edu using the FTP protocol.

forward (authenIP only)

Specifies screening rules that apply to packets that the firewall would normally forward (like a router) because their destinations are hosts other than the firewall itself.

The packet screening facility reads rules specified with the **authenIP** keyword before rules (including default Gauntlet firewall rules) specified with the **netconfig** keyword. The recommended way to add forward rules is through the packet screening editor in the administration tools.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
• authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny | absorb}-forward [-proto *protocol*] [-if *interface*] -srcaddr *address* -dstaddr *address* [-srcport *port*] [-dstport *port*]

permit-forward Packets are forwarded from one interface of the firewall to the other, as a router does.

deny-forward Packets are neither forwarded from one interface of the firewall to the other nor absorbed for processing as if they were addressed for the firewall. The firewall drops these packets.

absorb-forward The firewall accepts these packets as if their destination were the firewall itself and passes them on to the appropriate utility or proxy.

-proto *protocol*

The particular protocol for which this rule is valid. Valid values are defined in RFC 1700. Specify by protocol name or number. The wildcard * is valid.

You can specify a subset of the ICMP protocol.

Use the following syntax

.icmp: [!] *subtype* [& | | [!] *subtype*] [& | | [!] *subtype*]

where: *subtype* specifies one of subtypes of the ICMP protocol. Specify by subtype name.

Valid subtypes are:

ECHO

ECHOREPLY

IREQ

IREQREPLY

MASKREPLY

MASKREQ

PARAMPROB

REDIRECT

ROUTERADVERT

ROUTERSOLICIT

SOURCEQUENCH

TIMXCEED

TSTAMP

TSTAMPREPLY

UNREACH

! specifies that a particular subtype is not permitted.

& specifies multiple subtypes that are allowed.

| specifies that any of the listed subtypes are allowed.

-if *interface*

Name of the interface on which the packet arrives. Valid values vary by operating system and type of physical connection. The wildcard * is valid.

-srcaddr *address*
: Source IP address and netmask of the packet. The wildcard address 0.0.0.0:0.0.0.0 is valid.

-dstaddr *address*
: Destination IP address and netmask of the packet. The wildcard address 0.0.0.0:0.0.0.0 is valid.

-srcport *port*
: Source port of the packet by port number. The wildcard * is valid.

-dstport *port*
: Destination port of the packet by port number. The wildcard * is valid.

Example

```
authenIP: permit-forward -if ef1 -proto UDP -srcaddr
10.0.1.120:255.255.255.255 -dstaddr 10.0.1.33:255.255.255.255 -srcport
* -dstport 161
```

```
authenIP: permit-forward -if ef0 -proto UDP -srcaddr
10.0.1.33:255.255.255.255 -dstaddr 10.0.1.120:255.255.255.255 -srcport
* -dstport 161
```

The firewall forwards UDP packets (which can originate on any port) between an SNMP management station (10.0.1.120) on the trusted network and another workstation on the (204.255.154.27) untrusted network of the Gauntlet Intranet Firewall.

```
authenIP: permit-forward -if ef1 -proto icmp: !ROUTERADVERT |
!ROUTERSOLICIT -srcaddr 10.0.1.120:255.255.255.255 -dstaddr
10.0.1.33:255.255.255.255 -srcport * -dstport *
```

The firewall forwards all ICMP packets except ROUTERADVERT and ROUTERSOLICIT from a host on the trusted network (10.0.1.120) and a host on the untrusted network (10.0.1.33).

The commands *must* be on one line. They are wrapped here for readability.

Gauntlet Firewall Manager

Environment > Packet Screening tab > Add or Modify > Permit traffic to forward without any proxy application

function

Specifies particular functions of the protocol that are explicitly permitted or denied.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

ftp-gw: {permit | deny}-function *functions*

functions Specifies functions that are permitted or denied.

Valid values for the FTP proxy are:

- ABOR—Abort previous command
- ACCT—Specify account
- ALLO—Allocate storage
- APPE—Append to a file
- CDUP—Change to parent of current working directory
- CWD—Change working directory
- DELE—Delete a file
- HELP—Give help information
- LIST—List files in a directory

- MKD—Make directory
- MODE—Specify data transfer mode
- NLST—List names of files in directory
- NOOP—Do nothing
- PASS—Specify password
- PASV—Prepare for server-to-server transfer
- PORT—Specify data connection port
- PWD—Print the current working directory
- QUIT—Terminate session
- REIN—Full user terminate
- REST—Restart incomplete transfer
- RETR—Retrieve a file
- RMD—Remove a directory
- RNFR—Specify rename-from filename
- RNTO—Specify rename-to filename
- SITE—Nonstandard commands
- SIZE—Return size of a file
- SMNT—Structure mount
- STAT—Return status of server
- STOR—Store a file
- STOU—Store a file with a unique name
- STRU—Specify data transfer structure
- SYST—Show operating system server type
- TYPE—Specify data transfer type
- USER—Specify user name
- XCUP—Change to parent of current working directory
- XCWD—Change working directory

- XMKD—Make a directory
- XPWD—Print the current working directory
- XRMD—Remove a directory

Valid values for the HTTP proxy are:

- BINARY—Read Files
- DIR—List Directories
- EXEC—Exec Commands
- FTP—FTP Requests
- GOPHER—Gopher Requests
- HTTP—HTTP Requests
- HTTPREQ—HTTP Requests
- PLUS—Gopher+ Commands
- READ—Requests
- TEXT—Read Files
- TYPE—Content-type of header
- WAIS—Search Commands
- WRITE—Write Data

Example

```
ftp-gw: deny-function RETRs
```

The FTP proxy does not allow people to retrieve (RETR) files.

```
http-gw: deny-function FTP
```

The HTTP proxy does not allow FTP requests through the HTTP proxy.

Gauntlet Firewall Manager

Services > FTP tab > Operations

Services > HTTP tab > Add or Modify > Operations

groupid

Specifies the group ID the proxy uses when running.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	• strmwrks-gw
aol-gw	gui	• netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	• snmp-gw	• policy-*policy*
finger	• lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

groupid *group*

group Name of the group, either a name or numeric ID from the */etc/group* file.

Example

```
info-gw: groupid uucp
```

The Info Server runs using the group ID of uucp.

Gauntlet Firewall Manager

Services > Service tab > GroupID

handoff

Specifies the name of a host to which the FTP proxy or HTTP proxy hands the proxy request. This allows you to redirect FTP or HTTP requests to another system running an FTP or HTTP server, such as an anonymous FTP server running on your service net.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax for ftp-gw

ftp-gw: handoff *host[:port]*

host[:port] The host and port to which the FTP proxy forwards requests and the port on which it connects. Use IP addresses or hostnames. Specify port by service name or port number. If no port number is specified, the proxy uses port 21 by default.

Example

```
ftp-gw: handoff ftp.yoyodyne.com
```

The FTP proxy on the firewall hands all requests on port 21 to the FTP server (ftp.yoyodyne.com) running on the service network.

Gauntlet Firewall Manager

Services > FTP tab > Add or Modify > Handoff Host and Handoff Port

Syntax for http-gw

Specifies the name of a host to which the HTTP proxy hands the proxy request. This allows you to use several proxies, such as the HTTP proxy on the firewall and a caching proxy.

The HTTP proxy communicates with the next proxy as if it were a client rather than another proxy. You cannot use this setting in place of specifying the HTTP proxy in your browser. The handoff attribute does not work for FTP or Gopher URLs.

http-gw: handoff *host[:port]*

host[:port]	Specifies the host and port to which the HTTP proxy forwards requests and the port on which it connects. Use IP addresses or hostnames. Specify port by service name or port number. If no port number is specified, the proxy uses port 80 by default.

Example

```
http-gw: handoff fire-in.yoyodyne.com
```

The HTTP proxy on the firewall inside the network (*fw-engineering.engineering.yoyodyne.com*) hands all requests between the corporate network and the Internet (*fire-in.yoyodyne.com*) to the firewall.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Handoff Host and Handoff Port

header

Specifies HTTP headers that the proxy permits or denies. Denying a header causes the HTTP proxy to remove the related information from the request when it sends the header to the destination host.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

http-gw: {permit | deny}-header *header*

header Headers you wish to explicitly permit or deny (remove). You can specify only one header per line. Consult the HTTP 1.0/1.1 specifications for a list of headers. Certain headers are always processed by the HTTP proxy and are dealt with specifically:

- Connection
- Content-Length
- Content-Type
- Location
- Proxy-Connection

Example

```
http-gw: deny-header user-agent
http-gw: deny-header x-*
```

The HTTP proxy removes the user agent header and headers that begin with x- before sending the request to the destination host.

help-msg

Specifies the file that the proxy displays when the user accesses the *help* command.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

help-msg *file*

file Name of the file the proxy displays when the user accesses the *help* command. If no file is specified, the proxy displays a list of internal commands.

Example

```
rlogin-gw: help-msg /usr/local/etc/rlogin-help.txt
```

Displays the file */usr/local/etc/rlogin-help.txt* when a user requests access from the rlogin proxy.

Gauntlet Firewall Manager

Services > Service tab > Add or Modify > Help Message

hosts (authsrv only)

Specifies the hosts that can connect to the authentication server.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

authsrv: {permit | deny}-hosts *hosts*

hosts Hosts from which the authentication server accepts connections. Specify individual systems, entire networks, or subnets. Use IP addresses or hostnames. The wildcard * is valid.

Example

```
authsrv: permit-hosts 127.0.0.1
```

The authentication server accepts connections only from the firewall itself (localhost).

hosts (all but authsrv)

Specifies the hosts for which the proxy uses a particular policy, or the hosts that can use the proxy.

ahttp-gw	• gopher-gw	• mssql-gw	• RealAudio	• strmwrks-gw
• aol-gw	• gui	• netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	• info-gw	• NetShow	smap	• VDOLive
authsrv	• ldap-gw	• nntp-gw	smapd	• whois
• ck-gw	• lnotes-gw	pcxdpp	• snmpd	• x-gw
• cserve-gw	login-sh	• plug-gw	• snmp-gw	policy-*policy*
• finger	• lp-gw	• pop3-gw	• mbase-gw	
• ftp-gw	• mmp	• radm	• ssl-gw	

Syntax

{permit | deny}-*hosts* -policy *policy*

permit-hosts *hosts*

Hosts for which the proxy uses a particular policy, or hosts that can use the proxy.

deny-hosts *hosts*

Hosts that cannot use the proxy.

hosts	Hosts for which the proxy uses the particular policy. When used without the -**policy** option, indicates the hosts that can use the proxy. Specifies single hosts, entire networks, or subnets. Specify by IP address or hostname. The wildcard * is valid.
-policy *policy*	Name of the policy these hosts use.

Example

```
*: permit-hosts 10.0.4.* -policy restrictive
```

All requests from the network 10.0.4.* use the policy “restrictive”.

```
rsh-gw: permit-hosts 10.0.1.12
```

The host 10.0.1.12 can use the RSH proxy.

```
ftp-gw: deny-hosts 10.0.1.0:255.255.255.0
```

All the hosts on the 10.0.1.0:255.255.255.0 subnet cannot use the FTP proxy.

Gauntlet Firewall Manager

Firewall Rules > Rules tab

if-inside

Specifies the name and the IP address of the inside interface of the firewall. Used to create local screening rules that accept packets for the inside interface. Used to create forward screening rules that absorb packets if transparency is on.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	• netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	sql-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

if-inside -if *insideinterface* -addr *insideIPaddress*

insideinterface Interface name of the inside interface of the firewall. Valid values vary by operating system and type of physical connection.

InsideIPaddress IP address and subnet mask of the inside interface of the firewall.

Example

```
netconfig: if-inside -if le1 -addr 10.0.1.100:255.255.255.255
```

The inside interface of the firewall is le1 and the inside address of the firewall is 10.0.1.100.

Gauntlet Firewall Manager

Environment > IP Spoofing tab

if-outside

Specifies the name of an outside or service net interface and the IP address of the outside or service net interface of the firewall. Used to create local screening rules that accept packets for the outside interface.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	• netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

if-outside -if *outsideinterface* -addr *outsideIPaddress*

outsideinterface Interface name of the outside or service net interface of the firewall. Valid values vary by operating system and type of physical connection.

outsideIPaddress IP address and subnet mask of firewall's outside or service net interface.

Example

```
netconfig: if-outside -if we1 -addr 204.255.154.100:255.255.255.255
```

Firewall outside interface is we1, firewall the outside address is 204.255.154.100.

```
netconfig: if-outside -if we2 -addr 204.255.154.30:255.255.255.255
```

Firewall service net interface is we2, IP address of we2 is 204.255.154.30.

Gauntlet Firewall Manager

Environment > IP Spoofing tab

keepalive-timeout

Specifies the amount of time that the Gauntlet Firewall Manager waits for activity from the client before shutting itself down. If you do not use this attribute, the Gauntlet Firewall Manager waits 7200 seconds (2 hours) for activity before shutting itself down.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	• gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

keepalive-timeout *seconds*

seconds Number of seconds that the Gauntlet Firewall Manager waits for activity from the client before shutting itself down.

Example

```
gui: keepalive-timeout 1800
```

Gauntlet Firewall Manager waits 30 minutes (1800 seconds) before shutting itself down.

Gauntlet Firewall Manager

Environment > Firewall Access tab > Keep Alive

local

Specifies screening rules that apply to packets with a destination of the firewall itself.

Note that the packet screening facility reads rules specified with the **authenIP** keyword before rules (including default Gauntlet firewall rules) specified with the **netconfig** keyword. The recommended way to add local rules is through the packet screening editor in the administration tools.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
• authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-local [-proto *protocol*] [-if *interface*] -srcaddr *address* -dstaddr *address* [-srcport *port*] [-dstport *port*]

permit-local — The firewall accepts packets for local delivery and processing.

deny-local — The firewall does not accept packets for local delivery. The firewall drops these packets.

-proto *protocol* — Protocol for which this rule is valid. Valid values are specified in RFC 1770. Specify by protocol name or number. The wildcard * is valid.

-if *interface* Name of the interface on which the packet arrives. Valid values vary by operating system and type of physical connection. The wildcard * is valid.

-srcaddr *address*
Source IP address and netmask of the packet. The wildcard address 0.0.0.0:0.0.0.0 is valid.

-dstaddr *address*
Destination IP address and netmask of the packet. The wildcard address 0.0.0.0:0.0.0.0 is valid.

-srcport *port* Source port of the packet. Specify by port number. The wildcard * is valid.

-dstport *port* Destination port of the packet. Specify by port number. The wildcard * is valid.

Example

```
authenIP: deny-local -if ef0 -proto TCP
-srcaddr 192.168.1.0:255.255.255.0 -dstaddr 0.0.0.0:0.0.0.0 -srcport *
-dstport 25
```

The firewall denies all TCP connections on its outside interface (ef0) on port 25 (the SMTP port) from one network (192.168.1.0).

The command *must* be on one line. It is wrapped here for readability.

Gauntlet Firewall Manager

Environment > Packet Screening > Add or Modify > Deliver traffic locally to the firewall and Deny traffic

local-domain

Specifies the domains that are allowed to receive messages from anywhere. You always want your local domains to be able to receive mail from anywhere, so put all your domain names on this line.

This attribute and permit-relay (page 105) together provide the mailer with network knowledge about the domain. This helps the mailer guard against relay attacks, which

occur when an outside host connects to your mail port and uses your mailer to send mail from you to outside your network.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

smap: local-domain *domainnames*

domainnames Space-separated list of domain names.

Example

```
smap:local-domain fred.com celeste.com
```

Allows the local domains fred.com and celeste.com to receive messages from anywhere.

log

Specifies that proxies log only the operations listed, rather than all operations (the default). Note that the FTP proxy does not log all FTP operations by default. This attribute is equivalent to the **-log** command in previous versions.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	• lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

log *operations*

operations Specifies operations the proxies log. Refer to the function attribute (page 80) for a list of supported FTP functions.

Valid values for the HTTP proxy are:

- BINARY—Read files
- DIR—List directories
- EXEC—Exec commands
- FTP—FTP requests
- GOPHER—Gopher requests
- HTTP—HTTP requests
- HTTPREQ—HTTP requests
- PLUS—Gopher+ commands

- READ—Requests
- TEXT—Read files
- TYPE—Content-type of header
- WAIS—Search commands
- WRITE—Write data

Valid values for the lp proxy are:

- all
- print
- remove
- restart
- status-ln (long)
- status-sh (short)

Example

```
policy-trusted: log RETR STOR
```

The trusted policy logs only retrieve (RETR) and storage (STOR) activities.

Gauntlet Firewall Manager

Services > FTP tab > Operations

Services > HTTP tab > Add or Modify > Operations

You cannot set this attribute through the Gauntlet Firewall Manager for all proxies.

log (smap only)

Controls the anti-spam / anti-relay logging. If you don't put a log command in the smap portion of your netperm table, smap will not make a log entry whenever a spam or relay message is dropped.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

log spam-reject relay- reject

spam-reject Enables logging when spam messages are dropped.

relay-reject Enables logging when relays are dropped.

Example

```
smap: log relay-reject spam-reject
```

Enables logging for both relays and spam messages that are dropped.

manager

Specifies the manager that the SNMP proxy can contact.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	• snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

manager *manager* [port *agent-port*] [trap *trap-port*]

manager Name of the network manager that can use the proxy. Specify by IP address or hostname.

port *agent-port* Port on which the agent is listening for queries from the SNMP manager. If you do not include the *agent-port* option, the proxy uses port 161.

trap *trap-port* Port on which the proxy listens for trap messages from the agents. If you do not include the *agent-port* option, the proxy uses port 162.

Example

```
snmp-gw: manager 10.0.1.123
```

The network manager on 10.0.1.123 can use the SNMP proxy.

Gauntlet Firewall Manager

Services > SNMP tab > Manager's Network Address

maxbad

Specifies the number of incorrect consecutive login attempts a user can make before the authentication server disables the account.

If you do not use this attribute, the authentication server disables a user account after five unsuccessful login attempts.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

maxbad *logins*

logins Maximum number of incorrect login attempts a user can make before the authentication server disables the account.

Example

```
authsrv: maxbad 3
```

The authentication server allows three incorrect login attempts before disabling an account.

maxbytes

Specifies the maximum size (in bytes) of mail messages that the *smap* client accepts. After receiving the maximum number of bytes, the *smap* client truncates the message and sends the truncated message to the recipient. The *smap* client accepts the remaining data from the sender and discards it. If this attribute is not used, the *smap* client does not set a limit on the size of mail messages.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

maxbytes *bytes*

bytes Maximum size (in bytes) of mail messages that the *smap* client accepts.

Example

```
smap: maxbytes 2097152
```

The *smap* client accepts messages up to a size of 2 MB

maxchildren

Obsolete. Use the child-limit attribute (see “child-limit” on page 37.)

maxrecip

Specifies the maximum number of recipients that the *smap* client accepts in the SMTP dialog. If the SMTP dialog indicates that there are more recipients than allowed, then the *smap* client discards the message. The message is not delivered to anyone. If this attribute is not used, the smap client allows an unlimited number of recipients.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

maxrecip *recipients*

recipients Maximum number of recipients the smap client accepts in SMTP dialog.

Example

```
smap: maxrecip 25
```

The smap client accepts mail with a maximum of 25 recipients.

maxsessions

Specifies the maximum number of concurrent sessions that a single process of the HTTP proxy can support. When this limit is exceeded, the proxy creates a new process to handle the additional load.

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

maxsessions *sessions*

sessions Maximum number of concurrent sessions that a single process of the HTTP proxy can support.

Example

```
ahttp-gw: maxsessions 10
```

The authenticated HTTP proxy allows a maximum of ten concurrent sessions for a single process before creating a new process.

NetShow

Specifies the port on which the NetShow proxy listens for requests.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	• NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	• mmp	radm	ssl-gw	

Syntax

NetShow *port*

port Port on which the NetShow proxy listens for requests. Specify by port number or by port name as specified in */etc/services*.

Example

```
mmp: NetShow 1755
```

The NetShow proxy listens for requests on port 1755.

Gauntlet Firewall Manager

Services > NetShow tab > Ports

nobogus

Specifies that the authentication server indicates that a user ID does not exist when users attempt to log in and fail.

If this attribute is not specified and a user enters a nonexistent user name, the authentication server always responds with a bogus SNK challenge.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

nobogus true

Note: You must remove or comment out this setting if you wish to disable it. The settings "nobogus false" and "nobogus off" are not valid.

Example

```
authsrv: nobogus true
```

The authentication server indicates that the user ID does not exist (rather than displaying a bogus SNK challenge) when users attempt to log in and fail.

operation

Specifies explicitly permitted or denied operations for particular users or groups at particular times of day.

Note: The authentication server only uses these rules when the policy or the proxy uses the extended-permissions attribute (see "extended-permissions" on page 63.)

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

authsrv: {permit | deny}-operation [user *users* | group *groups*] *service destination* [*options*] [time *start end*]

permit-operation
: Operations to be permitted.

deny-operation
: Operations to be denied.

user *users*
: Specifies names of users for which the proxies use this rule. The wildcard * is valid.

group *groups*
: Names of groups for which the proxies use this rule. The wildcard * is valid.

service Name of a service for which this rule applies. Valid values are:

- ck-gw—circuit proxy
- ftp-gw—FTP proxy
- rlogin-gw—rlogin proxy
- rsh-gw—rsh proxy
- tn-gw—TELNET proxy
- *—all of these proxies

destination Hosts to which the proxies can or cannot send requests. Specify individual systems, entire networks, or subnets. Use IP addresses or hostnames. The wildcard * is valid.

options Specifies particular operations for each protocol that can be controlled. Valid values are:

- ck-gw—none
- ftp-gw—Consult the ftpd(1) man page
- rlogin-gw—none
- rsh-gw—none
- tn-gw—none

time *start* Time at which the proxy begins using this rule. Specify time in hours and minutes (between 00:00 and 23:59).

time *end* Time at which the proxy stops using this rule. Specify time in hours and minutes (between 00:00 and 23:59).

Example

```
authsrv: permit-operation group sales tn-gw * time 08:00 17:00
```

The sales group is permitted to use TELNET to connect to any destination only between the hours of 8:00 a.m. and 5:00 p.m.

```
authsrv: permit-operation user robert ftp-gw ftp.yoyodyne.com
```

The user robert is permitted to use FTP to connect only to ftp.yoyodyne.com.

Gauntlet Firewall Manager

Firewall Rules > Users tab > Restrictions
Services > Service tab > Add or Modify > Restrictions

ourname

Specifies the host and domain name that the graphical administrative tool or HTTP proxy uses when putting its own name into nontransparent forwarded URLs (links). Because the firewall may have different hostnames, this attribute allows you to specify which hostname to use.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	• gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

ourname *hostname*

hostname Name of the host that the GUI or HTTTP proxy uses when prepending URLs. Specify an individual interface. Use an IP address or hostname.

Example

```
gui: ourname 10.0.1.100
```

The GUI displays all pages as being on 10.0.1.100 (the inside interface of the firewall).

```
http-gw: ourname fire-in.yoyodyne.com
```

The HTTP proxy (if needed) prepends fire-in.yoyodyne.com (the inside interface of the firewall) to all URLs when rewriting them.

password change

Specifies password change options for allowing users to change passwords in authentication management system from within the TELNET and rlogin proxies.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-password change

permit	Hosts from which users can change their passwords. This is equivalent to the **-passok** option in previous versions
deny	Hosts from which users cannot change their passwords. Including a deny-password change rule has the same effect as not including those hosts in a permit-password change rule.

Example

```
policy-trusted: permit-password change
```

Allows users on the inside network to change their passwords from both the TELNET and rlogin proxies.

```
tn-gw: permit-password change
```

Allows users to change their passwords using the TELNET proxy. If this is the only `permit-password` change rule in the netperm table, users can only change their password from the TELNET proxy (not from the rlogin proxy).

Gauntlet Firewall Manager

Firewall Rules > Service Groups tab > Password Change

password-timeout

Specifies the amount of time between authentication requests. This attribute is useful if you are using a strong authentication system that uses one-time passwords, and you do not want to force your users to reauthenticate frequently. If you do not use this attribute, the proxy asks users to reauthenticate every 300 seconds (5 minutes).

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

password-timeout *seconds*

seconds Number of seconds between authentication requests by the proxy.

Example

```
ahttp-gw: password-timeout 1800
```

The authenticating HTTP proxy prompts users to reauthenticate every 30 minutes (1800 seconds).

peer-net

Specifies the IP address of networks that are part of the trusted network but are separated from the firewall by a bridge or a router. Use this attribute if you have multiple inside networks that you want to reach from hosts using PC Extender. If you do not use this attribute, hosts using PC Extender can only reach hosts on the network to which the firewall is directly connected.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	• pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

peer-net *network*

network Network that is part of the trusted network but is separated from the firewall by a bridge or a router. Specify by IP address. The * wildcard is valid.

Example

```
pcxdpp: peer-net 10.0.7.*
```

The PC Extender DPP daemon considers hosts on the 10.0.7.* to be peer networks.

Gauntlet Firewall Manager

Environment > Peer Networks tab > Add

permit-relay

Defines, one per line, the sites that are allowed to send relayed messages, that is, who is allowed to use your mail gateway to send mail anyway. You normally want all your own users to be able to send mail anywhere.

This attribute and local-domain (page 87) together provide the mailer with network knowledge about the domain. This helps the mailer guard against relay attacks, which occur when an outside host connects to your mail port and uses your mailer to send mail from you to outside your network.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

smap: permit-relay *domainname*

domainnames Domain name allowed to send relayed messages.

Example

```
smap:permit-relay fred.com
smap:permit-relay celeste.com
```

Allows the local domains fred.com and celeste.com to send relayed messages.

pop-server

Specifies the name of the system on which the POP3 server is running. This attribute is required for the POP3 proxy when you are using APOP authentication.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	• pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

pop-server *host*

host Name of the host on which the POP3 server is running (IP address or hostname).

Example

```
pop3-gw: pop-server mail
```

The POP3 proxy accesses the POP3 server running on the inside mail hub, mail.

Gauntlet Firewall Manager

Environment > Mail tab > POP3 > POP server location

port

Specifies the connection rule for this instance of the plug proxy, including hosts and ports.

ahttp-gw	gopher-gw	• mssql-gw	RealAudio	strmwrks-gw
• aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	• ldap-gw	• nntp-gw	smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	snmpd	x-gw
• cserve-gw	login-sh	• plug-gw	snmp-gw	policy-*policy*
• finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	• ssl-gw	

Syntax

port *port hosts* [-plug-to *hosts*] [-privport *] [-port *port*]

port	Name or port number, as specified in */etc/services*.
hosts	Hosts from which connections can originate: single hosts, entire networks, or subnets. Specify by IP address or hostname. The wildcard * is valid.
–plug-to *hosts*	Hosts to which the plug proxy connects: single hosts, entire networks, or subnets. Specify by IP address or hostname.
–privport	Proxy uses a reserved port number when connecting.
*	Provided for future extensibility.
–port *port*	Port on which the plug proxy connects on the remote host. Specify the name or port number, as specified in */etc/services*.

Example

```
qotd-gw: port qotd * -plug-to qotd.bigu.edu -port qotd
```

Creates a plug proxy rule for a Quote of the Day server (qotd-gw) which allows all hosts to connect to the Quote of the Day server at Big University on the *qotd* port.

Gauntlet Firewall Manager

Services > Plug tab > Add or Modify > Port

You cannot set this attribute through the Gauntlet Firewall Manager for all proxies.

ports

Specifies the ports on the destination host to which the proxy can connect. If you do not use this attribute, the proxy can connect to any port. Without this attribute, users can use the TELNET proxy to access any other network service that uses ASCII. This attribute is useful if you wish to ensure that the TELNET proxy is used only for accessing TELNET.

Without this attribute, users can designate a destination when they connect to an SSL server. This SSL connection connects to the remote service, which may or may not be running SSL. This attribute is useful if you wish to ensure that the HTTP proxy is used only to connect to standard SSL ports.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-ports *port-list*

permit-ports *port-list*
: List of ports to which the proxy can connect. Specify by port number or service name (as specified in */etc/services*). The wildcard * is valid. Use the ! character to deny a particular service.

deny-ports *port-list*
: List of ports to which the proxy cannot connect.

You cannot set this attribute through the Gauntlet Firewall Manager.

Example

```
tn-gw: permit-ports 4000
```

The TELNET proxy allows connections only to port 4000.

```
http-gw: permit-ports 8000 8080 ssl !*
```

The HTTP proxy allows connections only to a few common HTTP ports (8000 and 8080) and the SSL port (443) and denies connections to every other port (!*).

printer

Specifies a mapping from a client's print queue name to a server's host and print queue.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	• lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

printer *clientqueue* -host *server* -printer *serverqueue*

clientqueue Name of a client print queue.

–host *server* Server on which the remote printer queue is.

–printer *serverqueue*
Name of the remote printer queue to which a proxy sends the print jobs. If the server queue is not specified, the client's queue name is used as server queue name.

Example

```
lp-gw: printer lp_remote -host blaze.clientsite.com -printer lp3
```

Maps the printer queue lp_remote to the queue lp3, which is running on blaze.clientsite.com.

Gauntlet Firewall Manager

Services > LP tab > Add or Modify > Print Server and Server Queue

prompt

Specifies the prompt the proxies use in command mode.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	• x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

prompt *prompt*

prompt String that the proxy displays in command mode. Quotation marks are not required, but are recommended for strings that include spaces.

Example

```
tn-gw: prompt “Yoyodyne TELNET proxy> ”
```

The TELNET proxy displays the prompt “Yoyodyne TELNET proxy> ”.

Gauntlet Firewall Manager

Services > Service tab > Add or Modify > Command line prompt

proxy

Specifies proxy permissions.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-proxy *proxy-list*

permit-proxy — Proxies that this policy allows to run.

deny-proxy — Hosts that this policy does not allow to run. Including a deny-proxy rule has the same effect as not including those proxies in a permit-proxy rule.

proxy-list — Name of the proxy. This name must match the name specified in */usr/local/etc/mgmt/rc* or on the command line to start the proxy. If the proxy was started using the **-as** flag, use that name here.

Examples

```
policy-restrictive: permit-proxy ftp-gw http-gw
```

Allows the FTP and HTTP proxies to run.

```
policy-restrictive: permit-proxy webster
```

Allows a plug proxy configured for webster traffic to run.

Gauntlet Firewall Manager

Firewall Rules > Service Groups tab

quarantine-dir

Specifies the directory in which the *smapd* server places messages that fail the content scan. If you are using a content scanning engine to quarantine mail, you must specify this attribute.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

quarantine-dir *directory*

directory Directory in which the *smapd* server places messages that fail the content scan. Do not include a trailing slash (/). Ensure that this directory has the same owner and permission as the mail spool directory (as set by the directory attribute) that the *smapd* server uses.

Example

```
smapd: quarantine-dir /var/mail/quarantine
```

The *smapd* server places files that fail the content scan into the */var/mail/quarantine* directory.

Gauntlet Firewall Manager

Environment > Mail tab > Quarantine area

RealAudio

Specifies the port on which the RealAudio proxy listens for requests.

ahttp-gw	gopher-gw	mssql-gw	• RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	• mmp	radm	ssl-gw	

Syntax

RealAudio *port*

port Port on which the RealAudio proxy listens for requests. Specify by port number or by port name as specified in */etc/services*.

Example

```
mmp: RealAudio 7070
```

The RealAudio proxy listens for requests on port 7070.

Gauntlet Firewall Manager

Services > RealAudio tab > Ports

require-source

Specifies whether or not users of the X11 proxy, when starting the X11 proxy, must specify the name of the host from which they will be connecting.

If you do not use this attribute, users do not need to specify the name of the host when starting the X11 proxy.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	• x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

require-source { on | off }

Example

```
x-gw: require-source on
```

Users of the X11 proxy must specify the name of the host when starting the X11 proxy.

securidhost

Specifies the name of the firewall that is registered as the client hostname on the ACE/Server. Because the firewall may have various hostnames, this attribute allows you to specify which hostname to use.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

securidhost *firewall*

firewall Name of the firewall that is registered as the client hostname on the ACE/Server. Specify an individual system. Use an IP addresses or hostname.

Example

```
authsrv: securidhost fire-in.yoyodyne.com
```

The SecurID server communicates with the firewall's inside interface as fire-in.yoyodyne.com.

Gauntlet Firewall Manager

Environment -> Authentication -> SecurID -> Client host name

send-broken-post-requests

Specifies whether or not the HTTP proxy fixes broken POST requests by sending a carriage return/line feed after the data to the HTTP server.

If you do not use this attribute, the HTTP proxy requires that postings follow published specifications and does not send the carriage return/line feed. This may result in "Document contains no data" messages in your web browser.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

send-broken-post-requests { on | off }

Example

```
http-gw: send-broken-post-requests on
```

The HTTP proxy fixes broken POST requests by sending a carriage return/line feed after the data.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Fix broken POST requests

sendmail

Specifies an alternate path for *sendmail* or another mail delivery program you are using to deliver your mail inside your perimeter.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

sendmail *program*

program An alternate path for the *sendmail* executable or other program you are using to deliver mail.

Example

```
smapd: sendmail /usr/sbin/sendmail
```

The smapd server uses the *sendmail* executable in */usr/sbin/sendmail*.

Gauntlet Firewall Manager

Environment > Mail tab > SMAP > Alternate mail program

server

Specifies a server for which the proxy handles client/server connections.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

server *service* -port *remote-port* [-host *remote-host*] [-hostport *port*] [-timeout *minutes*] [-nookay]

server *service* Symbolic name for the service. Must be unique. Used by the proxy to create the menu of available services.

-port *remote-port*
Port on the remote host to which the circuit proxy connects. Specify by service name or port number.

-host *remote-host*
Name of the remote host to which the circuit proxy connects. Specify an individual system. Use IP address or hostname. This option is required if you are not using transparency.

-hostport *port* Port on which the proxy connects on the remote host.

-timeout *minutes*
: Number of minutes the client/server connection is idle before disconnecting for this service

-nookay
: Specifies that the proxy does not prompt the user to confirm before listening on the service port for a connection.

Example

```
ck-gw: server oracle -host db.clientsite.com -port oracle
```

The circuit proxy provides service for an Oracle server on the host db.clientsite.com.

Gauntlet Firewall Manager

Services > Circuit tab > Server Settings

shellfile

Specifies the name of the file in which the login shell finds information about users and their shells.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	• login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

shellfile *file*

file Name of the file that contains a list of users and their shells.

Example

```
login-sh: shellfile /usr/local/etc/login-shellfile
```

The login shell program looks in the */usr/local/etc/login-shellfile* file for information about users and their shells

snmp-manager

Specifies the IP address of the SNMP manager to which the SNMP agent on the firewall sends traps. If you do not use this attribute, the SNMP agent on the firewall does not send traps.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	• snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

snmp-manager *host*

host SNMP manager to which the SNMP agent on the firewall sends traps. Specify by IP address.

Example

```
snmpd: snmp-manager 10.0.1.58
```

The SNMP agent on the firewall sends traps to the SNMP manager running on the host 10.0.1.58.

Gauntlet Firewall Manager

Environment > SNMP Agent tab > SNMP Manager

system-contact

Specifies the information that the SNMP agent supplies as the contact when the network manager sends a request for the *system.sysContact* MIB-II variable. Use this attribute to provide information about the department to contact about the firewall. If you do not use this attribute, the firewall uses "Trusted Information Systems, Inc., +1 888 FIREWALL.""

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	• snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

system-contact *contact*

contact Information the SNMP agent supplies as the contact to the SNMP manager. If you use spaces in the contact, use quotation marks around the information.

Example

```
snmpd: system-contact “Systems Group 301-555-7135”
```

The SNMP agent sends the information “Systems Group 301-555-7135” when queried.

Gauntlet Firewall Manager

Environment > SNMP Agent tab > Contact

system-location

Specifies the information that the SNMP agent supplies about the location when the network manager sends a request for the *system.sysLocation* MIB-II variable. Use this attribute to provide information about the location of the firewall. If you do not use this attribute, the firewall sends “unknown.”

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	• snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

system-location *location*

location Information the SNMP agent supplies as the location to the SNMP manager. If you use spaces in the location, use quotation marks around the information.

Example

```
snmpd: system-location “Rockville: Third Floor: Room 468”
```

The SNMP agent sends the information “Rockville: Third Floor: Room 468” when queried.

Gauntlet Firewall Manager

Environment > SNMP Agent > Firewall Location

system-name

Specifies the information that the SNMP agent supplies about the name of the agent when the network manager sends a request for the *system.sysName* MIB-II variable. Use this attribute to provide information about the hostname of the firewall. If you do not use this attribute, the firewall sends its fully qualified domain name.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	• snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

system-name *name*

name Information the SNMP agent supplies as the location to the SNMP manager. Specify by hostname or IP address. If you use spaces in the name, use quotes around this information.

Example

```
snmpd: system-name “fire-in.yoyodyne.com”
```

The SNMP agent sends the information fire-in.yoyodyne.com when queried.

Gauntlet Firewall Manager

Environment > SNMP Agent > Firewall Name

tempdir

Specifies the directory in which the Authenticating HTTP proxy places its temporary files.

• ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

tempdir *directory*

directory Directory in which the Authenticating HTTP proxy places temporary files.

Example

```
ahttp-gw: tempdir /usr/tmp
```

The Authenticating HTTP directory places temporary files in the */usr/tmp* directory.

timeout

Specifies the amount of time the proxy is idle (with no network activity) before disconnecting. To disable the timeout feature for a proxy, do not set the timeout value to zero. Instead, set the timeout attribute to a large value, such as 10 years (315,360,000 seconds).

ahttp-gw	• gopher-gw	• mssql-gw	• RealAudio	• strmwrks-gw
• aol-gw	• gui	• netacl	• rlogin-gw	• syb-gw
alerts	• http-gw	netconfig	• rsh-gw	• tn-gw
authenIP	• info-gw	• NetShow	• smap	• VDOLive
authsrv	• ldap-gw	• nntp-gw	• smapd	• whois
ck-gw	• lnotes-gw	pcxdpp	• snmpd	• x-gw
• cserve-gw	login-sh	• plug-gw	• snmp-gw	• policy-*policy*
• finger	• lp-gw	• pop3-gw	• mbase-gw	
• ftp-gw	• mmp	radm	• ssl-gw	

Syntax

timeout *seconds*

seconds Number of seconds the proxy is idle before disconnecting.

Example

```
policy-trusted: timeout 1800
```

The trusted policy allows 1800 seconds (30 minutes) of idle time before the proxies disconnect.

Gauntlet Firewall Manager

Services > Service tab > Timeout

tmp-directory

Specifies the directory in which the *smapd* server creates temporary files during content scanning. If you do not use this attribute, the *smapd* server places temporary files in the */tmp* directory.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

tmp-directory *directory*

directory Directory in which the *smapd* server creates temporary files during content scanning. Do not include a trailing slash (/) character. Ensure that this directory has the same owner and permission as the mail spool directory (as set by the directory attribute) that *smapd* server uses. See "directory (gui, info-gw, smap and smapd only)" on page 59.

Example

```
smapd: tmp-directory /var/tmp/smapd
```

The *smapd* server creates temporary files in the */var/tmp/smapd* directory.

transparency

Specifies that the firewall uses inbound to outbound transparency. Used to create the packet screening rule in the forward rule set that absorbs packets from inside addresses to outside addresses for handling by the appropriate proxy or service.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	• netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

transparency {-on | - off}

-on Inbound to outbound transparency is on.

-off Inbound to outbound transparency is off.

Example

```
netconfig: transparency -on
```

Inbound to outbound transparency is on.

unknown

Specifies a list of names that the authentication server checks (in addition to the authentication database) when checking for extended permissions on a per user basis.

If the user name is not in the authentication database or in the list of names, the authentication server logs the attempt and indicates that the user is not valid. If the user name is found in the list of names, the authentication server assigns the user name to the group "unknown."

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
• authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

You cannot set this attribute through the Gauntlet Firewall Manager.

Syntax

permit-unknown *names*

names A list of names, separated by spaces. The wildcard * is valid.

Example

```
authsrv: permit-unknown scooter hikita penny
```

The authentication server considers scooter, hikita, and penny to be valid user names when it checks for extended permissions.

url

Lets you specify that certain URLs be denied to your users. If a user attempts to access a denied URL, the result is a message indicating that access to this URL is denied. You can use this feature to deny access to any URL whether or not you are using Cyber Patrol. If you are using Cyber Patrol, these denied sites are in addition to the sites denied by Cyber Patrol. You can also allow access to URLs that would otherwise be blocked by Cyber Patrol

Note that any URL to which you permit or deny access takes precedence over Cyber Patrol settings.

Use this attribute as part of a policy, rather than for the proxy itself.

See also the “cyber_masks” on page 49, “feature” on page 64, and “work_time” on page 142.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

policy-http-gw_Trusted: {permit | deny}-url *url*

permit-url URLs permitted for your users.

deny-url	URLs denied to your users.
url	An entire URL, or a substring of a URL: • .jpg matches all URLs with .jpg somewhere in the URL • yoyodyne.com matches all URLs with yoyodyne.com in the URL • ftp:// matches all URLs with ftp:// in the URL

Example

```
policy-http-gw_Trusted: permit-url yoyodyne.com
```

You want your users to be able to access any URL in the yoyodyne.com domain, even if Cyber Patrol has it blocked.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > URL Filtering

url-filter

Specifies characters that you want to deny in a URL.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

url-filter *filterlist*

filterlist xurl-encoded string of characters that you want to deny in a URL. See the HTML RFC or other HTML specification documents for lists of xurl-encoded characters.

Example

```
http-gw: url-filter %0D%0A
```

You do not want to see the carriage return/line feed characters in any URLs.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > URL Filtering

userid

Specifies the user ID the proxy uses when running. This attribute is equivalent to the `-user` command in previous versions.

ahttp-gw	• gopher-gw	mssql-gw	RealAudio	• strmwrks-gw
aol-gw	gui	• netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	• smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	• snmp-gw	• policy-*policy*
• finger	• lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

userid *user*

user Specifies the user as a name or a numeric ID from the */etc/passwd* file.

Example

```
smap, smapd: userid uucp
```

The *smap* and *smapd* processes run as the user uucp.

Gauntlet Firewall Manager

Services > Service tab > UserID

user-servers

Specifies the servers a particular user can access. Also specifies which services a particular users sees when using the circuit proxy menu.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

user-servers { user *user* | group *group* } [-deny] *service*

user *user*	Name of a user who can access a particular service.
group *group*	Name of a group who can access a particular service.
-deny	Specifies that the user can use all services except those explicitly denied.
service	Names of particular services. Must match the name of a service specified through a server attribute.

Example

```
ck-gw: user-servers group Grads accounting
```

The group Grads can use the accounting service.

Gauntlet Firewall Manager

Services > Circuit tab > User Settings

user-timeout

Specifies the amount of time the proxy is idle with no active client connections before disconnecting.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

user-timeout *minutes*

minutes Number of minutes the proxy is active with no client connections before disconnecting.

Example

```
ck-gw: user-timeout 10
```

The proxy waits ten minutes without an active client connection before disconnecting.

Gauntlet Firewall Manager

Services > Circuit tab > Add or Modify > User Timeout

VDOLive

Specifies the port on which the VDOLive proxy listens for requests.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	• VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	• mmp	radm	ssl-gw	

Syntax

VDOLive *port*

port Port on which the VDOLive proxy listens for requests. Specify by port number or by port name as specified in */etc/services*.

Example

```
mmp: VDOLive 7000
```

The VDOLive proxy listens for requests on port 7000.

Gauntlet Firewall Manager

Services > VDOLive tab > Port

virtual-net

Specifies how the DPP daemon tells the firewall to add rules to the kernel to implement transparency. If you do not use the virtual-net attribute, the firewall adds rules for each trusted host. If you use the virtual-net attribute, the DPP daemon tells the firewall to create rules for each virtual network that you specify. Using the virtual-net attribute, the DPP daemon no longer tells the firewall to create rules for a host if the host is part of the specified virtual network.

This attribute is optional.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	• pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

virtual-net *virtualnetworks* [-trusted]

virtualnetworks Virtual networks. Specify by IP address and netmask of the virtual network.

-trusted Specifies that the DPP daemon tells the firewall to create rules that indicate the virtual network is a trusted network.

Example

```
pcxdpp: virtual-net 10.0.10.0:255.255.255.0 -trusted
```

The DPP daemon tells the firewall to create one set of rules for the whole 10.0.10.* network, a trusted network.

Gauntlet Firewall Manager

Environment > Virtual Networks > Add

wakeup

Specifies the amount of time that the *smapd* server sleeps between scans of the spool directory for undelivered mail. If no value is specified, *smapd* uses a default value of 30 seconds.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	• smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

wakeup *seconds*

seconds Number of seconds that the *smapd* server sleeps between scans of the spool directory.

Example

```
smapd: wakeup 120
```

The *smapd* server sleeps for 120 seconds between scans.

Gauntlet Firewall Manager

Environment > Mail tab > SMAP > Wakeup frequency

welcome-msg

Specifies the file that the proxy displays as a welcome banner upon successful connection to the proxy.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
• ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
• ftp-gw	mmp	radm	ssl-gw	

Syntax

welcome-msg *file*

file Name of the file the proxy uses as a welcome banner upon successful connection to the proxy. If no file is specified, the proxy generates a default message.

Example

```
tn-gw: welcome-msg /usr/local/etc/tn-welcome.txt
```

Displays the file */usr/local/etc/tn-welcome.txt* when a user successfully connects to the TELNET proxy.

Gauntlet Firewall Manager

Services > Circuit tab > Welcome

Services > Service tab > Add or Modify Welcome Message

work_time

Lets you establish work (and leisure) time hours for the Cyber Patrol filtering software from Microsystems Software, which lets you block access to objectionable material.

This attribute has no effect unless Cyber Patrol is active. Refer to the *Gauntlet Firewall Administrator's Guide* for more information about Cyber Patrol.

Note: Leisure time hours are all hours outside of the defined work time hours.

See also the "cyber_masks" on page 49, "feature" on page 64, and "url" on page 132.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	rlogin-gw	syb-gw
alerts	• http-gw	netconfig	rsh-gw	tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

work_time *day_mask start_time end_time*

day_mask The bitmask of the day of the week or a range of days, from 00 to 7F. The bitmasks for the days of the week are:

- Sunday—0x01
- Monday—0x02
- Tuesday—0x04
- Wednesday—0x08
- Thursday—0x10
- Friday—0x20
- Saturday—0x40

To determine the bitmask for a range of days, use a hexadecimal calculator. To determine the bitmask for Monday through Friday, for example, enter **`02`** (for Monday), click OR, then enter **`04`** (for Tuesday), click OR again, and continue through **`20`** (for Friday) and click OR a final time. The result, `3E`, is the bitmask for Monday through Friday.

start_time The time of the day when *work_time* begins, using the twenty-four-hour system (sometimes called "military time"). For example, 0800 is 8 a.m. and 1700 is 5 p.m.

end_time The time of the day when *work_time* ends, using the twenty-four-hour system.

Example

```
http-gw: work_time 3E 800 0000
```

Work time hours are 8 a.m. to midnight Monday through Friday.

Gauntlet Firewall Manager

Services > HTTP tab > Add or Modify > Cyber Patrol > Define Work Times

xforwarder

Specifies the location of the executable to which the TELNET and rlogin proxies pass requests for the X proxy. Generally specifies the location of the X proxy.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

xforwarder *program*

program Location of the executable to which the TELNET and rlogin proxies pass requests for the X proxy.

Example

```
policy-trusted: xforwarder /usr/local/etc/x-gw
```

The TELNET and rlogin proxies use the standard X proxy for requests from the inside network.

Gauntlet Firewall Manager

Services > Service tab > Add or Modify > Xforwarder location

xgateway

Specifies X11 proxy permissions.

ahttp-gw	gopher-gw	mssql-gw	RealAudio	strmwrks-gw
aol-gw	gui	netacl	• rlogin-gw	syb-gw
alerts	http-gw	netconfig	rsh-gw	• tn-gw
authenIP	info-gw	NetShow	smap	VDOLive
authsrv	ldap-gw	nntp-gw	smapd	whois
ck-gw	lnotes-gw	pcxdpp	snmpd	x-gw
cserve-gw	login-sh	plug-gw	snmp-gw	• policy-*policy*
finger	lp-gw	pop3-gw	mbase-gw	
ftp-gw	mmp	radm	ssl-gw	

Syntax

{permit | deny}-xgateway *

permit	The TELNET and rlogin proxies can accept requests to start the X11 proxy.
deny	The TELNET and rlogin proxies do not accept requests to start the X11 proxy.
*	Provided for future extensibility.

Example

```
policy-trusted: permit-xgateway *
```

Allows the hosts on the inside network to start the X11 proxy.

Gauntlet Firewall Manager

Services > Service tab > Allow X11 requests

Chapter 5

Keyword Reference

This chapter lists each keyword and the attributes it can use. For more information about a specific attribute, refer to its description in Chapter 4, "Attribute Reference."

ahttp-gw

The **ahttp-gw** keyword supports the following attributes:

- authenticate
- authserver
- backend
- destination
- maxsessions
- password-timeout
- tempdir

aol-gw

The **aol-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address

- hosts
- port
- timeout

authenIP

The **authenIP** keyword supports the following attributes:

- forward
- local

authsrv

The **authserv** keyword supports the following attributes:

- accept-count
- badsleep
- bind-address
- child-limit
- database
- hosts
- maxbad
- nobogus
- operation
- securidhost
- unknown

ck-gw

The **ck-gw** keyword supports the following attributes:

- authenticate
- authserver
- circuitexec
- circuitsperuser
- circuit-timeout
- connect-timeout
- denial-msg
- destination
- directory
- extended-permissions
- groupid
- help-msg
- hosts
- password change
- prompt
- server
- userid
- user-servers
- user-timeout
- welcome-msg

cserve-gw

The **cserve-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

finger

The **finger** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

ftp-gw

The **ftp-gw** keyword supports the following attributes:

- accept-count
- authenticate
- authserver
- bind-address
- block
- child-limit
- content-failunsafe
- content-ftpchk
- contentscan-msg
- cvp-handling
- cvp-server
- data-port
- denial-msg
- denydest-msg
- destination
- directory
- extended-permissions
- functions
- groupid
- handoff
- help-msg
- hosts
- log
- timeout

- userid
- welcome-msg

gopher-gw

The **gopher-gw** keyword supports the following attributes:

- accept-count
- bind-address
- child-limit
- destination
- directory
- forward
- groupid
- hosts
- timeout
- userid
- url

gui

The **gui** keyword supports the following attributes:

- admin-user
- destination
- directory
- hosts
- keepalive-timeout
- ourname
- timeout

http-gw

The **http-gw** keyword supports the following attributes:

- accept-count
- anon-user
- authenticate
- bind-address
- child-limit
- content-failunsafe
- cvp-handling
- cvp-server
- cyber_masks
- denydest-msg
- destination
- directory
- feature
- forward
- function
- groupid
- handoff
- header
- hosts
- log
- ourname
- ports
- send-broken-post-requests
- timeout
- url

- url-filter
- userid
- work_time

info-gw

The **info-gw** keyword supports the following attributes:

- accept-count
- bind-inside
- child-limit
- destination
- directory
- hosts
- timeout

ldap-gw

The **ldap-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

lnotes-gw

The **lnotes-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

login-sh

The **login-sh** keyword supports the following attributes:

- authserver
- bind-address
- shellfile

lp-gw

The **lp-gw** keyword supports the following attributes:

- accept-count
- bind-inside
- child-limit
- client
- destination
- directory

- groupid
- hosts
- log
- mbase
- printer
- timeout
- userid

mbase-gw

The **mbase-gw** keyword supports the following attributes:

- check-server-ip
- child-limit
- force_source_address

mmp

The **mmp** keyword supports the following attributes:

- check-server-ip
- hosts
- NetShow
- RealAudio
- timeout
- VDOLive

mssql-gw

The **mssql-gw** keyword supports the following attributes:

- accept-count
- bind-inside
- child-limit
- destination
- hosts
- port
- timeout

netacl

The **netacl-gw** keyword supports the following attributes:

- bind-address
- child-limit
- destination
- directory
- groupid
- exec
- timeout
- userid

netconfig

The **netconfig** keyword supports the following attributes:

- bind-inside
- if-inside
- if-outside
- transparency

NetShow

The **NetShow** keyword supports the following attributes:

- check-server-ip
- destination
- hosts
- NetShow
- timeout

nntp-gw

The **nntp-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

pcxdpp

The **pcxdpp-gw** keyword supports the following attributes:

- authenticate
- database
- hosts
- peer-net
- virtual-net

plug-gw

The **plug-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

pop3-gw

The **pop3-gw** keyword supports the following attributes:

- accept-count
- authenticate
- authserver
- bind-address
- child-limit
- database
- destination
- groupid
- hosts
- pop-server
- timeout
- userid

radm

The **radm-gw** keyword supports the following attribute:

- hosts

RealAudio

The **RealAudio-gw** keyword supports the following attributes:

- check-server-ip
- destination
- hosts
- RealAudio
- timeout

rlogin-gw

The **rlogin-gw** keyword supports the following attributes:

- accept-count
- authenticate
- authserver
- bind-address
- child-limit
- denial-msg
- denydest-msg
- destination
- extended-permissions
- help-msg
- hosts
- password change
- prompt
- timeout
- welcome-msg
- xforwarder
- xgateway

rsh-gw

The **rsh-gw** keyword supports the following attributes:

- bind-address
- child-limit
- destination
- extended-permissions
- force_source_address
- hosts
- timeout
- userid

smap

The **smap** keyword supports the following attributes:

- deny-spam
- directory
- groupid
- local-domain
- log
- maxbytes
- maxrecip
- permit-relay
- timeout
- userid

smapd

The **smapd-gw** keyword supports the following attributes:

- badadmin
- baddir
- content-failunsafe
- cvp-handling
- cvp-server
- directory
- groupid
- maxbytes
- quarantine-dir
- sendmail
- timeout
- tmp-directory
- userid
- wakeup

snmpd

The **snmpd-gw** keyword supports the following attributes:

- hosts
- snmp-manager
- system-contact
- system-name
- system-location
- timeout

snmp-gw

The **snmp-gw** keyword supports the following attributes:

- agent
- child-limit
- destination
- groupid
- manager
- timeout
- userid

ssl-gw

The **ssl-gw** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

strmwrks-gw

The **strmwrks-gw** keyword supports the following attributes:

- destination
- directory
- groupid
- hosts
- timeout
- userid

syb-gw

The **syb-gw** keyword supports the following attributes:

- accept-count
- bind-inside
- child-limit
- destination
- hosts
- port
- timeout

tn-gw

The **tn-gw** keyword supports the following attributes:

- accept-count
- authenticate
- authserver
- bind-address
- child-limit

- denial-msg
- denydest-msg
- destination
- directory
- extended-permissions
- groupid
- help-msg
- hosts
- password change
- ports
- prompt
- timeout
- userid
- welcome-msg
- xforwarder
- xgateway

VDOLive

The **VODLive** keyword supports the following attributes:

- check-server-ip
- destination
- hosts
- timeout
- VDOLive

whois

The **whois** keyword supports the following attributes:

- accept-count
- bind-address
- buffer-size
- child-limit
- destination
- force_source_address
- hosts
- port
- timeout

x-gw

The **x-gw** keyword supports the following attributes:

- display
- hosts
- prompt
- require-source
- timeout

Index

A

accept-count, 20
activeX(permit/deny), 65
Administrator's Guide
  conventions, xxii
admin-user, 21
agent, 22
ahttp-gw keyword, 147
anon-user, 23
anonymous FTP server, 23
  handoff, 76
aol-gw keyword, 147
APOP authentication, 107
-auth option (previous version), 24
-authall option (previous version), 24
authenIP keyword, 148
authenticate, 24
authenticate(all but pcxdpp), 24
authenticate (pcxdpp only), 26
authentication server
  database path for APOP users, 53
  database path for PC Extender, 52
  database pathname, 52
  extended permissions, 63
  host, 80
  maxbad, 93
  names to check, 131
  nobogus, 98
  unknown, 131
authserver, 27
authserv keyword, 148
authtype *See, 28*

B

backend, 28
badadmin, 29
baddir, 30
badsleep, 31
banner, 46
bind-address, 32
bind-inside, 33
block, 34
buffer-size, 35

C

changing firewall configuration, 21
check-server-ip, 36
child-limit, 37
child processes, maximum, 37
circuitexec, 38
circuit proxy
  user access, 135
circuitsperuser, 39
circuit-timeout, 40
ck-gw keyword, 149

client, 41
client-server connections, maximum, 39
client to server transfer,blocking, 35
connect-timeout, 43
content-failunsafe, 44
content-ftpcheck, 45
content scan
  banner, 46
  failure message, 47
contentscan-msg, 46
conventions, xxii
cserve-gw keyword, 150
cvp-handling, 47
cvp-server, 48
cyber-mask, 49
Cyber Patrol
  blocked categories, 49
  leisure time, 142

D

database (authsrv only), 52
database (pcxdpp only), 53
database (pop3-gw only), 54
data-port, 51
denial-msg, 55, 57
denydest-msg, 56
deny-spam, 57
destination, 58
directory attribute, 59, 60
directory for undeliverable mail, 30
display, 61
DPP daemon, 25, 139

E

exec, 62
extended permissions, 131
extended-permissions, 63
  and operation, 99

F

failed logins, 31
feature, 64
finger, 63
finger keyword, 150
firewall,changing configuration, 21
force_source_address, 66
forking processes, 20
forward, 67
forward (authenIP only), 69
forward rules, 69
frames(permit/deny), 65
FTP
  anon-user, 23
  backend, 28
ftp-gw keyword, 151
FTP proxy
  block, 34
  content scan type, 45
  default logging, 89
  handoff, 76
  port 20 requirement, 51
function, 72

G

Gopher, backend, 28
gopher-gw keyword, 152

groupid, 75
gui keyword, 152

H

handoff, 76
  FTP or Gopher URLs, 77
header, 78
help-msg, 79
hosts, 81
hosts (authsrv only), 80
html2(permit/deny), 65
http-gw keyword, 153
HTTP proxy
  anon-user, 23
  backend, 28
  concurrent session maximum, 96
  denying features, 64
  forward, 67
  handoff, 77
  handoff to FTP or Gopher URLs, 77
  header, 78
  permitting features, 64
  POST request, 118
  temporary file, 127

I

ICMP protocol, 70
if-inside, 83
if-outside, 84
info-gw keyword, 154
inside interface, 83
internal buffer size, 35
IP address
  checking, 36
  force_source_address, 66
  inside interface, 83
  outside interface, 84
  peer-net, 104
  related to proxy, 32
IP spoofing, 33

J

java (permit/deny), 65

K

kanji (permit/deny), 65
keepalive-timeout, 85

L

ldap-gw keyword, 154
legacy-kanji(permit/deny), 65
lnotes-gw keyword, 155
local, 86, 88, 106
local-domain, 88
location information, 124
log, 89
log(smap only), 91
logins
  disallowed after failed, 31
  maximum incorrect, 93
login-sh keyword, 155
lp commands
  from client, 41
  log, 90
lp-gw keyword, 155

M

mail messages
  maximum recipients, 95
  maximum size, 94
  quarantine-dir, 114
  sendmail, 119
  undelivarable, 29, 30
manager, 91, 92
maxbad, 93
maxbytes, 94
maxchildren *See* child-limit, 95
maximum client/server connections, 39
maxrecip, 95
maxsessions, 96
mbase-gw keyword, 156
mmp keyword, 156
mssql-gw keyword, 157

N

netacl-gw keyword, 157
netconfig keyword, 158
netperm-table attributes
  accept-count, 20
  admin-user, 21
  agent, 22
  anon-user, 23
  authenticate, 24
  authenticate(all but pcxdpp), 24
  authenticate (pcxdpp only), 25
  authserver, 27
  backend, 28
  badadmin, 29
  baddir, 30
  badsleep, 31
  bind-address, 32
  bind-inside, 33
  block, 34
  buffer-size, 35
  check-server-ip, 36
  child-limit, 37
  circuitexec, 38
  circuitsperuser, 39
  circuit-timeout, 40
  client, 41
  connect-timeout, 43
  content-failunsafe, 44
  content-ftpcheck, 45
  contentscan-msg, 46
  cvp-handling, 47
  cvp-server, 48
  cyber-mask, 49
  database (authsrv only), 52
  database (pcxdpp only), 53
  data-port, 51
  denial msg, 55, 57
  denydest-msg, 56
  destination, 58
  directory(gui, info-gw, smap and smapd only), 59, 60
  display, 61
  exec, 62
  extended-permissions, 63
  feature, 64
  force_source_address, 66
  forward, 67
  forward (authenIP only), 69
  function, 72
  groupid, 75
  handoff, 76
  header, 78
  help-msg, 79
  host(authsrv only), 80
  hosts, 81
  if-inside, 83
  if-outside, 84
  keepalive-timeout, 85
  local, 86, 88, 106

log, 89
manager, 91, 92
maxbad, 93
maxbytes, 94
maxrecip, 95
maxsessions, 96
NetShow, 97
nobogus, 98
operation, 99
ourname, 101
password change, 102
password-timeout, 103
peer-net, 104
pop-server, 107
port, 108
ports, 109
printer, 111
prompt, 112
proxy, 113
quarantine-dir, 114
RealAudio, 115
require-source, 116
securidhost, 117
send-broken-post-requests, 118
sendmail, 119
server, 120
shellfile, 121
snmp-manager, 122
system-contact, 123
system-location, 124
system-name, 126
tempdir, 127
timeout, 128
tmp-directory, 129
transparency, 130
unknown, 131
url, 132
url-filter, 133
userid, 134
user-servers, 135
user-timeout, 137
virtual-net, 139
VODLive, 138
wakeup, 140
welcome-msg, 141
work_time, 142
xforwarder, 144
xgateway, 145
NetShow, 97
NetShow keyword, 158
network management agent, 22
nntp-gw keyword, 158
nobogus, 98

O

operation, 99
outname, 101
outside interface, 84

P

packet screening edito, 69
passok option *See* passok, 102
password, 23
password_change, 102
password-timeout, 103
PC Extender, 26
peer-net, 104
pcxdpp-gw keyword, 159
peer-net, 104
permissions
extended permissions, 63
See denial-msd, denydest-msg, destination
permit-relay, 106
plug-gw keyword, 159
plug proxy

force_source_address, 66
port, 108
pop3-gw keyword, 160
POP3 proxy pop-server, 107
pop-server, 107
port, 108
ports, 109
POST request, 118
printer, 111
processes
maximum number of child processes, 37
per connection, 20
prompt, 112
proxies
group ID, 75
internal buffer size, 35
related IP address, 32
root directory(gui, info-gw, smap and smapd only), 59, 60
proxy, 113

Q

quarantine-dir, 114

R

radm-gw keyword, 160
RealAudio, 115
RealAudio-gw keyword, 160
relayed messages, 88, 106
relay-reject, 91
require-source, 116
RETR, 90
RFC, 70
rlogin-gw, 161
rlogin proxy password change, 102
root directory, 59, 60
rsh-gw, 162

S

screening rules
firewall destination packets, 86
for outside interface, 84
script(permit/deny), 65
securidhost, 117
send-broken-post-requests, 118
sendmail, 119
server, 120
server to client transfer, blocking, 35
shellfile, 121
smap
relayed messages, 106
smapd-gw, 163
SMAPD server
badadmin, 29, 30
wakeup, 140
smap keyword, 162
SMAP proxy
sendmail, 119
SMAP server
temporary files, 129
SMTP proxy
maximum recipients, 95
SNK, 98
SNMP agent
contact information, 123
firewall host name, 126
location information, 124
snmpd-gw, 163
snmp-gw, 164

snmp-manager, 122
SNMP proxy
  contact agent, 22
  manager, 92
spam-reject, 91
ssl-gw, 164
STOR, 90
strmwrks-gw, 165
strong authentication
  password-timeout, 103
syb-gw, 165
system-contact, 123
system-location, 124
system-name, 126

T

TELNET proxy
  password change, 102
  TELNET access, 109
tempdir, 127
time-out
  before showdown, 85
  client/server connection, 40
  connect-timeout, 43
timeout, 128
tmp-directory, 129
tn-gw, 165
transparency, 130
trusted network, 33
turning off IP checking, 36

U

UDP, 71
undeliverable mail, 29, 30
unknown, 131
url, 132
url-filter, 133
URL prepending, 101
user for undeliverable mail, 29
userid, 134
user-servers, 135
user-timeout, 137

V

virtual-net, 139
VODLive, 138
VODLive keyword, 166

W

wakeup, 140
welcome banner, 46
welcome message
  contentscan-msg, 46
  welcome-msg, 141
welcome-msg, 141
whois keyword, 167
wildcard characters
  authenIP, 71
  client, 42
  cvp-server, 48
  peer-net, 105
  port-list, 110
  unknown, 131
work_time, 142

X

X11 proxy
  permissions, 145
  require source, 116
  xforwarder, 144
xforwarder, 144
xgateway, 145
x-gw keyword, 167
xurl-encoded string to be denied, 134

Tell Us About This Manual

As a user of Silicon Graphics products, you can help us to better understand your needs and to improve the quality of our documentation.

Any information that you provide will be useful. Here is a list of suggested topics:

- General impression of the document
- Omission of material that you expected to find
- Technical errors
- Relevance of the material to the job you had to do
- Quality of the printing and binding

Please send the title and part number of the document with your comments. The part number for this document is 007-3822-003.

Thank you!

Three Ways to Reach Us

- To send your comments by **electronic mail**, use either of these addresses:
  - On the Internet: techpubs@sgi.com
  - For UUCP mail (through any backbone site): *[your_site]*!sgi!techpubs
- To **fax** your comments (or annotated copies of manual pages), use this fax number: 650-932-0801
- To send your comments by **traditional mail**, use this address:

  Technical Publications
  Silicon Graphics, Inc.
  2011 North Shoreline Boulevard, M/S 535
  Mountain View, California 94043-1389