**Block for client1**

**,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,**

#yum install squid

# vim /etc/squid/squid.conf

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

54 http\_access deny client-blocked client

55 #http\_access deny blocked\_sites hpcsalab

56 http\_access allow hpcsalab

57 # from where browsing should be allowed

58 #http\_access allow localnet

59 http\_access allow localhost

60

61 # And finally deny all other access to this proxy

62 http\_access deny all

63

64 # Squid normally listens to port 3128

65 http\_port 3128

66

67 # Uncomment and adjust the following to add a disk cache directory.

68 cache\_dir ufs /var/spool/squid 2048 16 256

69 visible\_hostname proxy.hpcsa.lab

70 # Leave coredumps in the first cache dir

71 coredump\_dir /var/spool/squid

72

73 #

74 # Add any of your own refresh\_pattern entries above these.

75 #

76 refresh\_pattern ^ftp: 1440 20% 10080

77 refresh\_pattern ^gopher: 1440 0% 1440

78 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

79 refresh\_pattern . 0 20% 4320

,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,

#Vim /etc/squid/client1-blocked.txt

.redhat.com

.cisco.com

.Youtube.com

.Microsoft.com

* Now on client machine browser [www.redhat.com](http://www.redhat.com) , [www.youtube.com](http://www.youtube.com) all these website will not browse it is blocked

-------------------------------------------------------------------------------------------------------------------------------------------------------

**Block for window-client**

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

55 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

56 http\_access deny window-blocked window

57 http\_access deny client-blocked client

58 #http\_access deny blocked\_sites hpcsalab

59 http\_access allow hpcsalab

60 # from where browsing should be allowed

61 #http\_access allow localnet

62 http\_access allow localhost

63

64 # And finally deny all other access to this proxy

65 http\_access deny all

66

67 # Squid normally listens to port 3128

68 http\_port 3128

69

70 # Uncomment and adjust the following to add a disk cache directory.

71 cache\_dir ufs /var/spool/squid 2048 16 256

72 visible\_hostname proxy.hpcsa.lab

73 # Leave coredumps in the first cache dir

74 coredump\_dir /var/spool/squid

75

76 #

77 # Add any of your own refresh\_pattern entries above these.

78 #

79 refresh\_pattern ^ftp: 1440 20% 10080

80 refresh\_pattern ^gopher: 1440 0% 1440

81 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

82 refresh\_pattern . 0 20% 4320

#vim /etc/squid/window-blocked.txt

.wikipedia.org

.esakal.com

.centos

.yahoo

* Now on window machine browser Wikipedia.org , esakal.com,centos,yahoo all these website will not browse it is blocked

-------------------------------------------------------------------------------------------------------------------------------------------------------

**Block for network**

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

55 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

56 acl hpcsalab-blocked dstdomain "/etc/squid/blocked.txt"

57 http\_access deny hpcsalab-blocked hpcsalab

58 http\_access deny window-blocked window

59 http\_access deny client-blocked client

60 #http\_access deny blocked\_sites hpcsalab

61 http\_access allow hpcsalab

62 # from where browsing should be allowed

63 #http\_access allow localnet

64 http\_access allow localhost

65

66 # And finally deny all other access to this proxy

67 http\_access deny all

68

69 # Squid normally listens to port 3128

70 http\_port 3128

71

72 # Uncomment and adjust the following to add a disk cache directory.

73 cache\_dir ufs /var/spool/squid 2048 16 256

74 visible\_hostname proxy.hpcsa.lab

75 # Leave coredumps in the first cache dir

76 coredump\_dir /var/spool/squid

77

78 #

79 # Add any of your own refresh\_pattern entries above these.

80 #

81 refresh\_pattern ^ftp: 1440 20% 10080

82 refresh\_pattern ^gopher: 1440 0% 1440

83 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

84 refresh\_pattern . 0 20% 4320

#vim /etc/squid/blocked.txt

.wikipedia.org

.esakal.com

.centos

.yahoo

-------------------------------------------------------------------------------------------------------------------------------------------------------

**Allow following web sites between 2pm to 5pm**

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl hpcsa-time time A 14:00-17:00

55 acl hpcsa dstdomain "/etc/squid/time-blocked.txt"

56 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

57 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

58 acl hpcsalab-blocked dstdomain "/etc/squid/blocked.txt"

59 http\_access deny hpcsa hpcsa-time

60 http\_access deny hpcsalab-blocked hpcsalab

61 http\_access deny window-blocked window

62 http\_access deny client-blocked client

63 #http\_access deny blocked\_sites hpcsalab

64 http\_access allow hpcsalab

65 # from where browsing should be allowed

66 #http\_access allow localnet

67 http\_access allow localhost

68

69 # And finally deny all other access to this proxy

70 http\_access deny all

71

72 # Squid normally listens to port 3128

73 http\_port 3128

74

75 # Uncomment and adjust the following to add a disk cache directory.

76 cache\_dir ufs /var/spool/squid 2048 16 256

77 visible\_hostname proxy.hpcsa.lab

78 # Leave coredumps in the first cache dir

79 coredump\_dir /var/spool/squid

80

81 #

82 # Add any of your own refresh\_pattern entries above these.

83 #

84 refresh\_pattern ^ftp: 1440 20% 10080

85 refresh\_pattern ^gopher: 1440 0% 1440

86 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

87 refresh\_pattern . 0 20% 4320

-------------------------------------------------------------------------------------------------------------------------------------------------------

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl hpcsa-time time A 14:00-17:20

55 acl hpcsa dstdomain "/etc/squid/time-blocked.txt"

56 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

57 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

58 acl hpcsalab-blocked dstdomain "/etc/squid/blocked.txt"

59 http\_access allow hpcsa hpcsa-time

60 http\_access deny hpcsalab-blocked hpcsalab

61 http\_access deny window-blocked window

62 http\_access deny client-blocked client

63 #http\_access deny blocked\_sites hpcsalab

64 http\_access allow hpcsalab

65 # from where browsing should be allowed

66 #http\_access allow localnet

67 http\_access allow localhost

68

69 # And finally deny all other access to this proxy

70 http\_access deny all

71

72 # Squid normally listens to port 3128

73 http\_port 3128

74

75 # Uncomment and adjust the following to add a disk cache directory.

76 cache\_dir ufs /var/spool/squid 2048 16 256

77 visible\_hostname proxy.hpcsa.lab

78 # Leave coredumps in the first cache dir

79 coredump\_dir /var/spool/squid

80

81 #

82 # Add any of your own refresh\_pattern entries above these.

83 #

84 refresh\_pattern ^ftp: 1440 20% 10080

85 refresh\_pattern ^gopher: 1440 0% 1440

86 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

87 refresh\_pattern . 0 20% 4320

###############################################################################################

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl hpcsa-time time A 14:00-17:20

55 acl hpcsa dstdomain "/etc/squid/time-blocked.txt"

56 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

57 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

58 acl hpcsalab-blocked dstdomain "/etc/squid/blocked.txt"

59 http\_access allow hpcsa hpcsa-time

60 http\_access deny hpcsa !hpcsa-time -----------------------> this is used to not allow after the given time period

61 http\_access deny hpcsalab-blocked hpcsalab

62 http\_access deny window-blocked window

63 http\_access deny client-blocked client

64 #http\_access deny blocked\_sites hpcsalab

65 http\_access allow hpcsalab

66 # from where browsing should be allowed

67 #http\_access allow localnet

68 http\_access allow localhost

69

70 # And finally deny all other access to this proxy

71 http\_access deny all

72

73 # Squid normally listens to port 3128

74 http\_port 3128

75

76 # Uncomment and adjust the following to add a disk cache directory.

77 cache\_dir ufs /var/spool/squid 2048 16 256

78 visible\_hostname proxy.hpcsa.lab

79 # Leave coredumps in the first cache dir

80 coredump\_dir /var/spool/squid

81

82 #

83 # Add any of your own refresh\_pattern entries above these.

84 #

85 refresh\_pattern ^ftp: 1440 20% 10080

86 refresh\_pattern ^gopher: 1440 0% 1440

87 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

88 refresh\_pattern . 0 20% 4320

-------------------------------------------------------------------------------------------------------------------------------------------------------

Allow these words only on client director pc

crikcet,football,ipl,movies,bookmtshow

1 #

2 # Recommended minimum configuration:

3 #

4

5 # Example rule allowing access from your local networks.

6 # Adapt to list your (internal) IP networks from where browsing

7 # should be allowed

8 acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

9 acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

10 acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

11 acl localnet src fc00::/7 # RFC 4193 local private network range

12 acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

13

14 acl SSL\_ports port 443

15 acl Safe\_ports port 80 # http

16 acl Safe\_ports port 21 # ftp

17 acl Safe\_ports port 443 # https

18 acl Safe\_ports port 70 # gopher

19 acl Safe\_ports port 210 # wais

20 acl Safe\_ports port 1025-65535 # unregistered ports

21 acl Safe\_ports port 280 # http-mgmt

22 acl Safe\_ports port 488 # gss-http

23 acl Safe\_ports port 591 # filemaker

24 acl Safe\_ports port 777 # multiling http

25 acl CONNECT method CONNECT

26

27 #

28 # Recommended minimum Access Permission configuration:

29 #

30 # Deny requests to certain unsafe ports

31 http\_access deny !Safe\_ports

32

33 # Deny CONNECT to other than secure SSL ports

34 http\_access deny CONNECT !SSL\_ports

35

36 # Only allow cachemgr access from localhost

37 http\_access allow localhost manager

38 http\_access deny manager

39

40 # We strongly recommend the following be uncommented to protect innocent

41 # web applications running on the proxy server who think the only

42 # one who can access services on "localhost" is a local user

43 #http\_access deny to\_localhost

44

45 #

46 # INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS

47 #

48

49 # Example rule allowing access from your local networks.

50 # Adapt localnet in the ACL section to list your (internal) IP networks

51 acl hpcsalab src 10.10.10.0/24

52 acl client src 10.10.10.130

53 acl window src 10.10.10.132

54 acl hpcsa-time time A 14:00-17:20

55 acl hpcsa dstdomain "/etc/squid/time-blocked.txt"

56 acl client-blocked dstdomain "/etc/squid/client1-blocked.txt"

57 acl badwords url\_regex -i "/etc/squid/director-blocked.txt"

58 acl window-blocked dstdomain "/etc/squid/window-blocked.txt"

59 acl hpcsalab-blocked dstdomain "/etc/squid/blocked.txt"

60 http\_access allow hpcsa hpcsa-time

61 http\_access allow badwords client

62 http\_access deny badwords !client

63 http\_access deny hpcsa !hpcsa-time

64 http\_access deny hpcsalab-blocked hpcsalab

65 http\_access deny window-blocked window

66 http\_access deny client-blocked client

67 #http\_access deny blocked\_sites hpcsalab

68 http\_access allow hpcsalab

69 # from where browsing should be allowed

70 #http\_access allow localnet

71 http\_access allow localhost

72

73 # And finally deny all other access to this proxy

74 http\_access deny all

75

76 # Squid normally listens to port 3128

77 http\_port 3128

78

79 # Uncomment and adjust the following to add a disk cache directory.

80 cache\_dir ufs /var/spool/squid 2048 16 256

81 visible\_hostname proxy.hpcsa.lab

82 # Leave coredumps in the first cache dir

83 coredump\_dir /var/spool/squid

84

85 #

86 # Add any of your own refresh\_pattern entries above these.

87 #

88 refresh\_pattern ^ftp: 1440 20% 10080

89 refresh\_pattern ^gopher: 1440 0% 1440

90 refresh\_pattern -i (/cgi-bin/|\?) 0 0% 0

91 refresh\_pattern . 0 20% 4320

~