Secured Branch Router Configuration Example

Contents

Introduction

This document provides a sample configuration for securing a branch router by implementing the following features:

- **Context-Based Access Control (CBAC)**—CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when specified traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if the traffic is part of the same session as the original traffic that triggered CBAC when exiting through the firewall.
- **Cisco IOS Intrusion Prevention System (IPS)**—The Cisco IOS IPS feature restructures the existing Cisco IOS Intrusion Detection System (IDS), allowing customers to choose to load the default, built-in signatures or to load a Signature Definition File (SDF) called *attack-drop.sdf* onto the router. The attack-drop.sdf file contains 118 high-fidelity Intrusion Prevention System (IPS) signatures, providing customers with the latest available detection of security threats.
- **Cisco IOS Firewall Authentication Proxy**—Authentication proxy provides dynamic, per-user authentication and authorization, authenticating users against industry standard TACACS+ and RADIUS authentication protocols. Per-user authentication and authorization of connections provide more robust protection against network attacks.

Cisco Systems

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

- **Firewall Websense URL Filtering**—The Firewall Websense URL Filtering feature enables your Cisco IOS firewall (also known as Cisco Secure Integrated Software) to interact with the Websense URL filtering software, thereby allowing you to prevent users from accessing specified websites on the basis of some policy. The Cisco IOS firewall works with the Websense server to know whether a particular URL should be allowed or denied (blocked).

Before You Begin

Conventions

For more information on document conventions, see *Conventions Used in Cisco Technical Tips*.

Components Used

The information in this document is based on the software and hardware versions below.

- Cisco 2801 router
- Cisco IOS Release 12.3(8)T4
- Advanced IP Services feature set

Note The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Related Products

This configuration can also be used with the following hardware:

- Cisco 1800 series integrated services router (modular)
- Cisco 2800 series integrated services router
- Cisco 3800 series integrated services router

A similar configuration can also be used with a Cisco 3800 series integrated services router that is equipped with a Cisco Content Engine network module (NM-CE-BP), which has an embedded Websense URL filtering server (UFS).

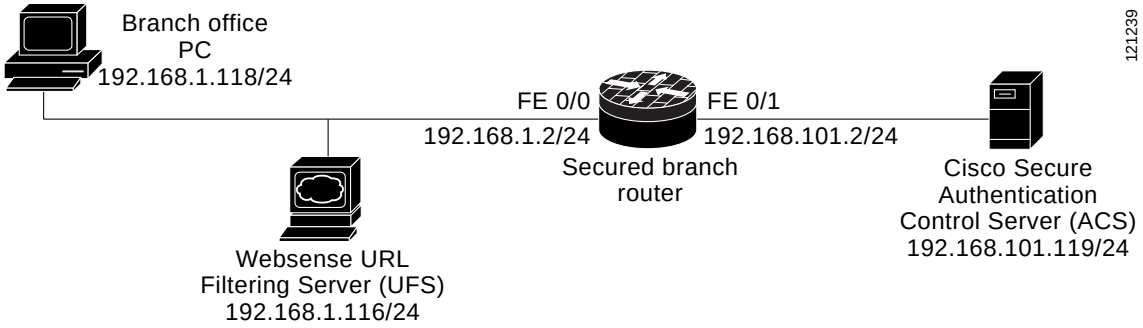
Configure

In this section, you are presented with the information to configure the features described in this document.

Tip To find additional information on the commands used in this document, use the Command Lookup Tool. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Network Diagram

This document uses the network setup shown in the diagram below.



Not shown in the diagram is an HTTP server with IP address 192.168.102.119/24. The HTTP server may be located anywhere in the network. In this case, it is on the Fast Ethernet 0/1 side of the secured branch router.

Configurations

This document uses the configuration shown below.

```
router# show running-config
Building configuration...
.
.
.
!---Enable the authentication, authorization, and accounting (AAA) access control model.
aaa new-model
!
!---Identify the Cisco Secure Authentication Control Server (ACS) as a member of a
!---AAA server group. In this example, the AAA server group is called "SJ."
aaa group server tacacs+ SJ
 server 192.168.101.119
!
!---Enable AAA authentication at login and specify the authentication methods to try.
aaa authentication login default local group SJ none
```

```
!---Restrict user access to the network:
!---(a) Run authorization to determine if the user is allowed to run an EXEC shell.
!---(b) Enable authorization that applies specific security policies on a per-user basis.
!---You must use the "aaa authorization auth-proxy" command together with the
!---"ip auth-proxy <name>" command (later in this configuration). Together, these
!---commands set up the authorization policy to be retrieved by the firewall.
aaa authorization exec default group SJ none
aaa authorization auth-proxy default group SJ
!---Make sure that the same session ID is used for each AAA accounting service type
!---within a call.
aaa session-id common
.
.
.
!---Define a set of inspection rules. In this example, the set is called "myfw."
!---Include each protocol that you want the Cisco IOS firewall to inspect.
ip inspect name myfw cuseeme timeout 3600
ip inspect name myfw ftp timeout 3600
ip inspect name myfw http urlfilter timeout 3600
ip inspect name myfw rcmd timeout 3600
ip inspect name myfw realaudio timeout 3600
ip inspect name myfw smtp timeout 3600
ip inspect name myfw sqlnet timeout 3600
ip inspect name myfw streamworks timeout 3600
ip inspect name myfw tftp timeout 30
ip inspect name myfw udp timeout 15
ip inspect name myfw tcp timeout 3600
ip inspect name myfw vdolive
!
!---(Optional) Set the length of time an authentication cache entry, along with its
!---associated dynamic user access control list, is managed after a period of inactivity.
ip auth-proxy inactivity-timer 120
!---Create an authentication proxy rule; in this example it is named "aprule."
!---Set HTTP to trigger the authentication proxy.
ip auth-proxy name aprule http
!
!---Configure the Cisco IOS Intrusion Protection System (IPS) feature:
!---Specify the location from which the router loads the Signature Definition File (SDF).
!---(Optional) Specify the maximum number of event notifications that are placed
!---in the router's event queue.
!---Disable the audit of any signatures that your deployment scenario deems unnecessary.
!---Name the IPS rule, so that you can apply the rule to an interface.
!---Later in this example, this rule (named "ids-policy") is applied to FE 0/0.
ip ips sdf location tftp://192.168.1.3/attack-drop.sdf
ip ips po max-events 100
ip ips signature 1107 0 disable
ip ips signature 3301 0 disable
ip ips name ids-policy
!
!---Configure the Firewall Websense URL Filtering feature:
!---(Optional) Set the maximum number of destination IP addresses that can be cached
!---into the cache table, which consists of the most recently requested IP addresses
!---and respective authorization status for each IP address.
!---Specify domains for which the firewall should permit or deny all traffic
!---without sending lookup requests to the Firewall Websense URL filtering server (UFS).
!---Specify the IP address of the Firewall Websense UFS.
ip urlfilter cache 0
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter server vendor websense 192.168.1.116
.
.
.
```

```
!---Configure the firewall interface that connects to the branch office PCs
!---and the Firewall Websense UFS:
!---Apply access lists and inspection rules to control access to the interface.
!---In this example, access list 116 is used to filter outbound packets, and
!---the inspection rule named "myfw" is used to filter inbound packets.
!---Enable the authentication proxy rule for dynamic, per-user authentication
!---and authorization. See the previous "aaa authorization auth-proxy default group SJ"
!---and "ip auth-proxy name aprule http" command entries.
!---Apply the Cisco IPS rule to outbound traffic.
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.0
 ip access-group 116 out
 ip inspect myfw in
 ip auth-proxy aprule
 ip ips ids-policy out
.
.
.
!---Configure the interface that connects to the
!---Cisco Secure Authentication Control Server (Cisco Secure ACS).
!---Apply access lists to control access to the interface.
!---In this example, access list 111 is used to filter inbound packets.
interface FastEthernet0/1
 ip address 192.168.101.2 255.255.255.0
 ip access-group 111 in
.
.
.
ip classless
!---The following command establishes a static route to the HTTP server,
!---which in this example has an IP address of 192.168.102.119.
ip route 192.168.102.0 255.255.255.0 FastEthernet0/1
!
!---Enable the HTTP server on your system.
!---Also, specify that the authentication method used for AAA login service
!---should be used for authenticating HTTP server users.
ip http server
ip http authentication aaa
no ip http secure-server
!
!---Configure the access list for the interface that connects to the
!---Cisco Secure ACS.
access-list 111 permit tcp host 192.168.101.119 eq tacacs host 192.168.101.2
access-list 111 permit udp host 192.168.101.119 eq tacacs host 192.168.101.2
access-list 111 permit icmp any any
access-list 111 deny   ip any any
!
!---Configure the access list for the firewall interface that connects to the
!---branch office PCs and the Websense URL Filtering Server (UFS).
access-list 116 permit tcp host 192.168.1.118 host 192.168.1.2 eq www
access-list 116 deny   tcp host 192.168.1.118 any
access-list 116 deny   udp host 192.168.1.118 any
access-list 116 deny   icmp host 192.168.1.118 any
access-list 116 permit tcp 192.168.1.0 0.0.0.255 any
access-list 116 permit udp 192.168.1.0 0.0.0.255 any
access-list 116 permit icmp 192.168.1.0 0.0.0.255 any
!
!
```

```
!---Specify the Cisco Secure ACS, in this case a TACACS+ server.
!---Set the authentication encryption key used for all TACACS+ communications
!---between the access server and the TACACS+ daemon. This key must match the key
!---used on the TACACS+ daemon.
tacacs-server host 192.168.101.119
tacacs-server directed-request
tacacs-server key cisco
!
.
.
.
end
```

Verify

This section provides information you can use to confirm your configuration is working properly:

- Commands for Verifying Firewall Websense URL Filtering, page 6
- Commands for Verifying Cisco IOS Firewall Authentication Proxy, page 7
- Commands for Verifying Context-Based Access Control, page 7
- Commands for Verifying Cisco IOS Intrusion Prevention System, page 8

Tip Certain **show** commands are supported by the Output Interpreter Tool, which allows you to view an analysis of **show** command output. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click Cancel at the login dialog box and follow the instructions that appear.

Commands for Verifying Firewall Websense URL Filtering

- **show ip urlfilter cache**—Displays the maximum number of entries that can be cached into the cache table and the number of entries and the destination IP addresses that are cached into the cache table.

```
Router# show ip urlfilter cache

Maximum number of cache entries: 0
Number of entries cached: 0
-----------------------------------------------------------
    IP address        Age         Time since last hit
                  (In seconds)     (In seconds)
-----------------------------------------------------------
```

- **show ip urlfilter config**—Displays the configured vendor servers, including the size of the cache, the maximum number of outstanding requests, and the allow mode state.

```
Router# show ip urlfilter config
Websense URL Filtering is ENABLED

Primary Websense server configurations
======================================
Websense server IP address Or Host Name: 192.168.1.116
Websense server port: 15868
Websense retransmission time out: 6 (in seconds)
Websense number of retransmission: 2
```

```
Secondary Websense servers configurations
=========================================
Other configurations
====================
Allow Mode: OFF
System Alert: ENABLED
Audit Trail: DISABLED
Log message on Websense server: DISABLED
Maximum number of cache entries: 0
Maximum number of packet buffers: 200
Maximum outstanding requests: 1000
```

- **show ip urlfilter statistics**—Displays URL filtering statistics, such as the number of requests that are sent to the Websense server, the number of responses received from the Websense server, the number of pending requests in the system, the number of failed requests, and the number of blocked URLs.

```
Router# show ip urlfilter statistics

URL filtering statistics
========================
Current requests count: 0
Current packet buffer count(in use): 0
Current cache entry count: 0

Maxever request count: 0
Maxever packet buffer count: 0
Maxever cache entry count: 0

Total requests sent to URL Filter Server :13
Total responses received from URL Filter Server :13
Total requests allowed: 9
Total requests blocked: 4
```

Commands for Verifying Cisco IOS Firewall Authentication Proxy

- **show ip auth-proxy**—Displays the authentication proxy entries or configuration.

```
Router# show ip auth-proxy cache

Authentication Proxy Cache
 Client Name admin, Client IP 192.168.1.118, Port 1902, timeout 120, Time Remaining
120, state INIT

Router# show ip auth-proxy statistics

configuration
Authentication global cache time is 120 minutes
Authentication global absolute time is 0 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Rule Configuration
 Auth-proxy name aprule
    http list not specified auth-cache-time 120 minutes
```

Commands for Verifying Context-Based Access Control

- **show ip access-list**—Displays the contents of current IP access lists.
- **show ip inspect session**—Displays CBAC session information.

Commands for Verifying Cisco IOS Intrusion Prevention System

- **show ip ips signature**—Displays Cisco IPS signature information, including which signatures are disabled and marked for deletion.

```
Router# show ip ips signature

Signatures were last loaded from tftp://192.168.1.3/attack-drop.sdf

SDF release version not available

*=Marked for Deletion  Action=(A)larm,(D)rop,(R)eset   Trait=AlarmTraits
MH=MinHits             AI=AlarmInterval                CT=ChokeThreshold
TI=ThrottleInterval    AT=AlarmThrottle                FA=FlipAddr
WF=WantFrag            Ver=Signature Version

Signature Micro-Engine: SERVICE.SMTP (1 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  3129:0      Y   ADR   MED     0      0     0     0    15 FA  N    S59

Signature Micro-Engine: SERVICE.RPC (29 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  6100:0      Y   AD   HIGH     0      0     0   100    30 FA  N    1.0
  6100:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    1.0
  6101:0      Y   AD   HIGH     0      0     0   100    30 FA  N    1.0
  6101:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    1.0
  6104:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6104:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6105:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6105:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6188:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S43
  6189:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S43
  6189:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S43
  6190:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6190:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6191:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6191:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6192:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  6192:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.1
  6193:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6193:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6194:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6194:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6195:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  6195:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    2.2
  6196:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S4
  6196:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S4
  6197:0      Y   ADR  HIGH     0      0     0   100    30 FA  N    S9
  6197:1      Y   AD   HIGH     0      0     0   100    30 FA  N    S9
  6276:0      Y   AD   HIGH     0      0     0   100    30 FA  N    S30
  6276:1      Y   ADR  HIGH     0      0     0   100    30 FA  N    S30

Signature Micro-Engine: SERVICE.HTTP (23 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  3140:3      Y   ADR  HIGH     0      1     0     0    15 FA  N    S80
  3140:4      Y   ADR  HIGH     0      1     0     0    15 FA  N    S80
  5045:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
  5047:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
  5055:0      Y   AD   HIGH     0      1     0     0    15 FA  N    2.2
  5071:0      Y   ADR  HIGH     0      1     0     0    15 FA  N    2.2
```

```
 5081:0      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:0      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:1      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5114:2      Y   ADR   MED     0      1      0      0    15 FA  N    2.2
 5126:0      Y   ADR   MED     0      1      0      0    15 FA  N    S5
 5159:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S7
 5184:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:1      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:2      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5188:3      Y   ADR  HIGH     0      1      0      0    15 FA  N    S12
 5245:0      Y   ADR   MED     0      1      0      0    15 FA  N    S21
 5326:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S30
 5329:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    1.0
 5364:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S43
 5390:0      Y   ADR   MED     0      1      0      0    15 FA  N    S54
 5400:0      Y   ADR  HIGH     0      1      0      0    15 FA  N    S71

Signature Micro-Engine: ATOMIC.TCP (42 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ---------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
 3038:0      Y   AD   HIGH     0      0      0    100    30 FA  N  Y 2.2
 3039:0      Y   AD   HIGH     0      0      0    100    30 FA  N  Y 2.2
 3040:0      Y   AD   HIGH     0      0      0    100    30 FA  N  N 2.2
 3041:0      Y   AD   HIGH     0      0      0    100    30 FA  N  N 2.2
 3043:0      Y   AD   HIGH     0      0      0    100    30 FA  N  Y 2.2
 3300:0      Y   AD   HIGH     0      0      0    100    30 FA  N    2.1
 9200:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9201:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9202:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9203:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9204:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9205:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9206:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9207:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9208:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9209:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9210:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9211:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9212:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9213:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9214:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9215:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9216:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9217:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9218:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9223:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S40
 9224:0      Y   AD    MED     0      0      0    100    30 FA  N    S44
 9225:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9226:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9227:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9228:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9229:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9230:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S46
 9231:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S66
 9232:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S69
 9233:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S67
 9236:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S71
 9237:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S71
 9238:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S71
 9239:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S76
 9240:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S79
 9241:0      Y   AD   HIGH     0      0      0    100    30 FA  N    S82
```

```
Signature Micro-Engine: ATOMIC.IPOPTIONS (1 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  1006:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1

Signature Micro-Engine: ATOMIC.L3.IP (4 sigs)
 SigID:SubID On Action  Sev Trait     MH    AI    CT    TI AT FA WF Ver
 ----------- -- ------ ---- -----  ----- ----- ----- ----- -- -- -- ---
  1102:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.1
  1104:0      Y   AD   HIGH     0      0     0   100    30 FA  N    2.2
  1108:0      Y   AD   HIGH     0      0     0   100    30 GS  N    S27
  2154:0      Y   AD   HIGH     0      0     0   100    30 FA  N  Y 1.0
Total Active Signatures: 118
Total Inactive Signatures: 0
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

See the following documents:

- *Troubleshooting CBAC Configurations*, tech note
- *Troubleshooting Authentication Proxy*, tech note

Troubleshooting Commands

Note Before issuing **debug** commands, please see *Important Information on Debug Commands*.

- **debug ip inspect**—Displays messages about Cisco IOS firewall events.
- **debug ip urlfilter**—Enables debug information of URL filter subsystems.

```
Router# debug ip urlfilter detailed

Urlfilter Detailed Debugs debugging is on
Router#
*Aug 26 20:11:58.538: URLF: got cache idle timer event...
*Aug 26 20:11:58.538: URLF: cache table is about to overflow, delete idle entries
*Aug 26 20:12:00.962: URLF: creating uis 0x64EF00A0, pending request 1
*Aug 26 20:12:00.962: URLF: domain name not found in the exclusive list
*Aug 26 20:12:00.962: URLF: got an cbac queue event...
*Aug 26 20:12:00.962: URLF: websns making a lookup request.
*Aug 26 20:12:00.962: URLF: socket send successful...
*Aug 26 20:12:00.962: URLF: holding pak 0x64823210 (192.168.101.119:80) ->
192.168.1.118:1087 seq 3905567052 wnd 17238
*Aug 26 20:12:00.966: URLF: got a socket read event...
*Aug 26 20:12:00.966: URLF: socket recv (header) successful.
*Aug 26 20:12:00.966: URLF: socket recv (data) successful.
*Aug 26 20:12:00.966: URLF: websns lookup code = 1
*Aug 26 20:12:00.966: URLF: websns lookup description code = 1027
*Aug 26 20:12:00.966: URLF: websns category number = 67
*Aug 26 20:12:00.966: URLF: websns cache command = 0
*Aug 26 20:12:00.966: URLF: websns cached entry type = 0
*Aug 26 20:12:00.966: URLF: Site/URL Blocked: sis 0x64A57D50, uis 0x64EF00A0
*Aug 26 20:12:00.966: URLF: Sent Deny page with FIN to client and RST to server
```

```
*Aug 26 20:12:00.966: URLF: urlf_release_http_resp_for_url_block - Discarding the pak
0x64823210 held in resp Q (count 1 : thrld 200)
*Aug 26 20:12:00.966: URLF: deleting uis 0x64EF00A0, pending requests 0
```

- **debug ip auth-proxy**—Displays authentication proxy activity.

```
Router# debug ip auth-proxy detailed

*Aug 30 23:16:07.680: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.680:  SYN SEQ 24350097 LEN 0
*Aug 30 23:16:07.680: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.680: AUTH-PROXY:auth_proxy_half_open_count++ 1
*Aug 30 23:16:07.684: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.684:  ACK 2787182962 SEQ 24350098 LEN 0
*Aug 30 23:16:07.684: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.684: clientport 1900 state 0
*Aug 30 23:16:07.684: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.684:  PSH ACK 2787182962 SEQ 24350098 LEN 282
*Aug 30 23:16:07.684: dst_addr 192.168.102.119 src_addr 192.168.1.118 dst_port 80
src_port 1900
*Aug 30 23:16:07.684: clientport 1900 state 0
*Aug 30 23:16:07.688: AUTH-PROXY:proto_flag=4, dstport_index=4
*Aug 30 23:16:07.688:  ACK 2787184131 SEQ 24350380 LEN 0
```

Related Information

- *Cisco IOS Security Configuration Guide*, Release 12.3:
  - "Configuring Context-Based Access Control" chapter
  - "Configuring Authentication Proxy" chapter
- *Cisco IOS Intrusion Prevention System (IPS)*, Cisco IOS Release 12.3(8)T feature module
- *Firewall Websense URL Filtering*, Cisco IOS Releases 12.2(11)YU and 12.2(15)T feature module
- *Troubleshooting CBAC Configurations*, tech note
- *Troubleshooting Authentication Proxy*, tech note
- Technical Support—Cisco Systems