Cisco ISR G2 and Cloud Web Security Troubleshooting Guide

Design Guide

September, 2014

Contents

Introduction 3

Connectivity to the CWS Tower 3

Verifying Connectivity 3
Distinguishing Between ISR G2 and CWS Tower Issues 4
License Issues 8

CWS Functionality 9

Mismatched Time Zones 10
User Authentication Failures 10
Session Flows 12

User Experience 15

Introduction

This document offers tips for resolving common errors that may occur with the Cisco® Integrated Service Routers (ISR) Generation 2 (G2) with Cisco Cloud Web Security (CWS). It is assumed that the reader is familiar with the ISR G2 and the CWS Connector that runs on the router. It is also assumed that CWS has already been configured on the ISR G2 and proper licensing has been obtained for the CWS ScanCenter portal.

For more information on the ISR web security solution with CWS, refer to the Cisco ISR with Cisco Cloud Web Security Solution Guide.

Before proceeding with troubleshooting, make sure the ISR G2 has the latest CWS-supported Cisco IOS® image installed with a K9 security license and proper Internet connectivity and routing. Cisco IOS images may be downloaded from the Download Software page on Cisco.com. To verify installed licenses, issue the **show version** or **show license** command on the router's command-line interface.

The following sections cover connectivity from the ISR G2 to the CWS tower, CWS functionality, and the user experience. These sections build on each other, and troubleshooting should be performed in the order of these sections. Issues in one section should be resolved before moving on to the next.

Connectivity to the CWS Tower

Cisco Cloud Web Security will not operate properly if the ISR G2 router cannot reach the CWS tower. This section will help determine whether the ISR G2 has connectivity to the CWS tower and offers possible steps for resolution if the tower is not reachable.

Verifying Connectivity

To verify connectivity to the tower, issue the command **show content-scan summary**. As seen below, if connectivity is established with the CWS tower, you should see the word **(Up)** in parentheses.

```
router#show content-scan summary
Primary: 72.37.244.115 (Up)*
Secondary: 80.254.152.99 (Up)
Interfaces: FastEthernet4
```

If instead you are seeing **(Down)** for one of the towers, the router most likely does not have connectivity to that tower.

```
router#show content-scan summary
Primary: 72.37.244.115 (Down)*
Secondary: 80.254.152.99 (Down)
Interfaces: FastEthernet4
```

You can also use Telnet to try to connect to the CWS tower directly. Connect to the IP address of the tower with the port number that you specified in your configuration. An **Open** message means you have connectivity to the tower; if Telnet times out and disconnects, there is no connectivity.

```
! Connectivity between ISR G2 and Cloud Web Security Tower
router#telnet 72.37.244.115 8080
Trying 72.37.244.115, 8080 ... Open
! No connectivity between ISR G2 and Cloud Web Security Tower
router#telnet 72.37.244.115 8080
Trying 72.37.244.115, 8080 ...
% Connection timed out; remote host not responding
```

Next Steps

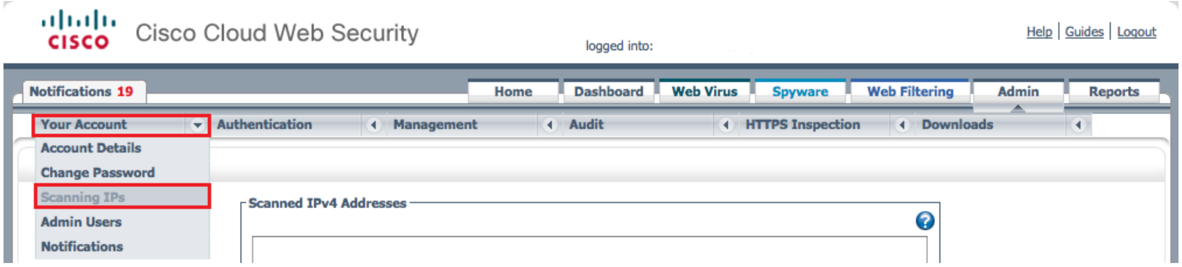
- Check your routing to make sure your network is able to reach the CWS tower.
- Make sure no firewalls are blocking access to the tower.
- If you need support, open a case with the Cisco Technical Assistance Center (TAC).

Distinguishing Between ISR G2 and CWS Tower Issues

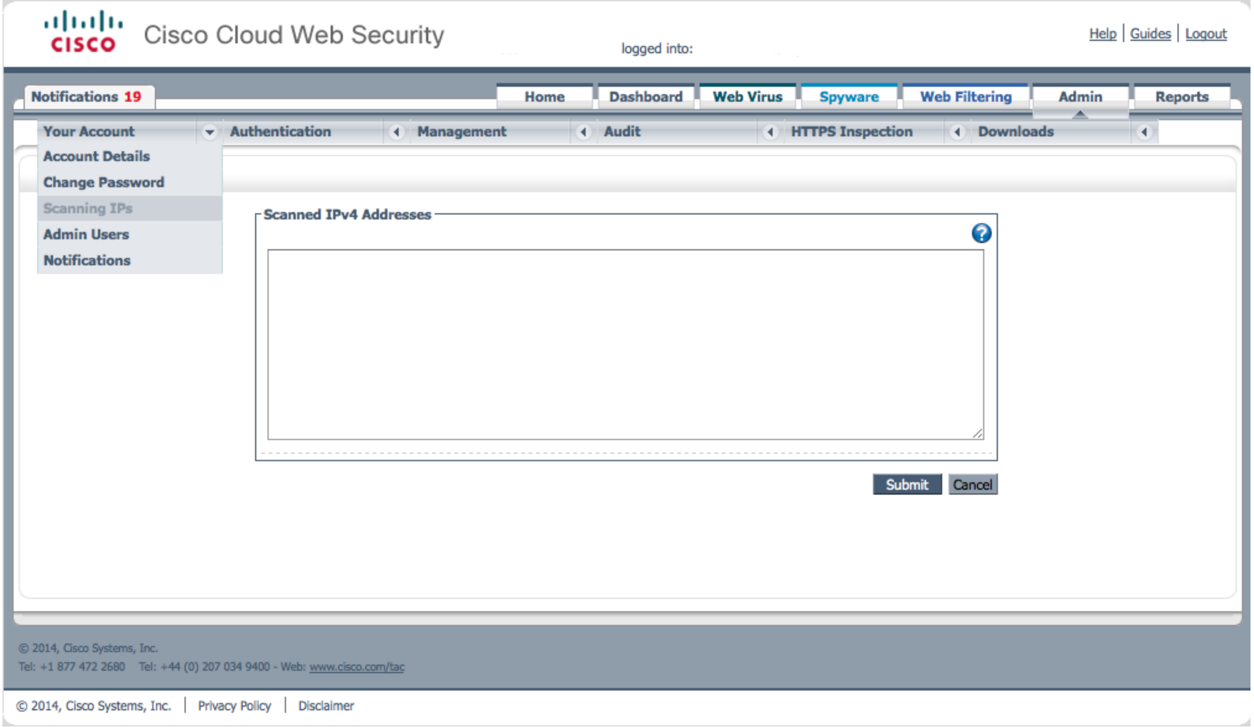
If you have verified that both towers are up and you are able to connect to them with Telnet, but you are getting blank pages when browsing, try to determine whether the issue is with the ISR G2 or the CWS tower. If you open a support case, you will receive a faster resolution if you report the case to the proper contact (on the ISR G2 side or the CWS side). To determine the origin of a problem, configure the tower IP directly on the browser proxy settings to bypass the ISR G2. This will help you determine whether you have a router issue or a tower issue.

Because you will be bypassing the ISR G2 and not using the license configured on it, the tower will not recognize you as an authorized user. To allow the CWS tower to still recognize the traffic as authorized, you must first add your egress IP address to the list of scanning IPs in CWS. You can find your egress IP address by going to www.whatismyip.com on your laptop or client. The example below shows how to add the egress IP address to CWS's list of scanning IPs.

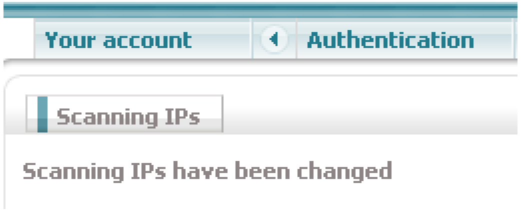
1. In the CWS interface, click the Admin tab, and in the Your Account menu, select Scanning IPs.



2. Enter the egress IP address in the list with the subnet mask, and click Submit.



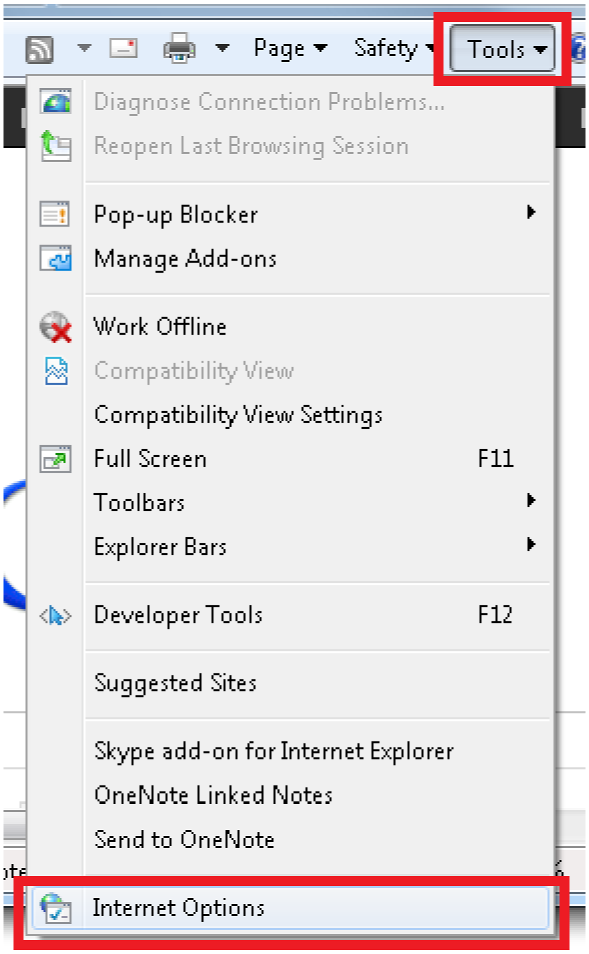
3. You will get a confirmation message that the Scanning IPs have been changed.



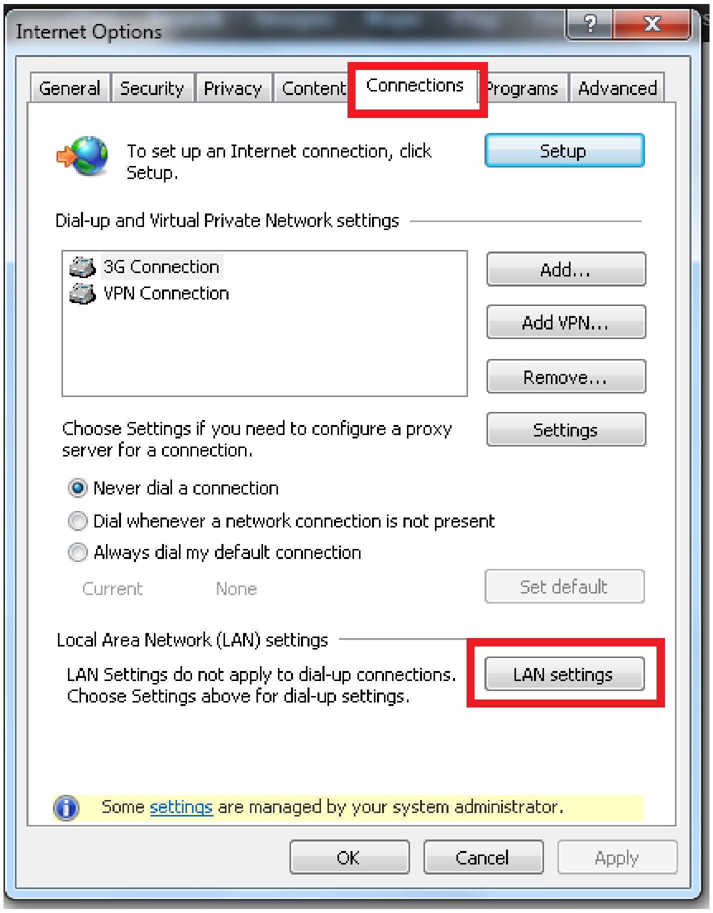
Scanning IPs have been changed

The following example shows how to configure a proxy with Internet Explorer. The steps may vary in other browsers.

1. In IE, go to Tools → Internet Options



2. In the Connections tab, click LAN settings.



Internet Options

General | Security | Privacy | Content | Connections | Programs | Advanced

To set up an Internet connection, click Setup. [Setup]

Dial-up and Virtual Private Network settings

3G Connection
VPN Connection

[Add...] [Add VPN...] [Remove...]

Choose Settings if you need to configure a proxy server for a connection. [Settings]

● Never dial a connection
○ Dial whenever a network connection is not present
○ Always dial my default connection

Current None [Set default]

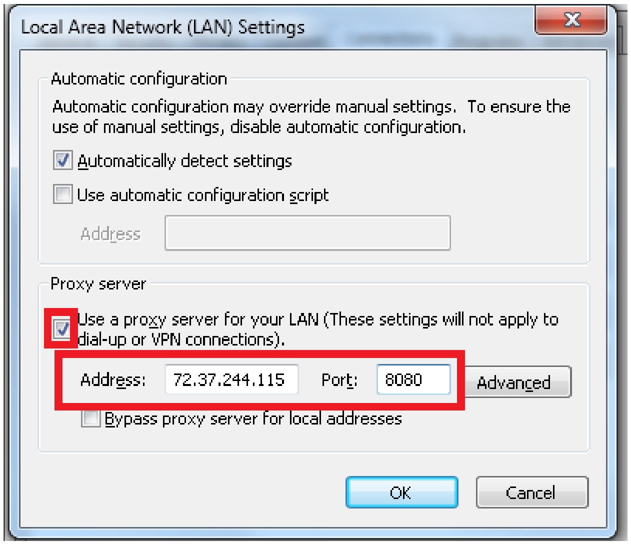
Local Area Network (LAN) settings

LAN Settings do not apply to dial-up connections. Choose Settings above for dial-up settings. [LAN settings]

Some settings are managed by your system administrator.

[OK] [Cancel] [Apply]

3. In the Proxy server section, select the “Use a proxy server for your LAN” checkbox. Enter the IP address of the CWS tower in the Address field and the port number in the Port field, and click OK when done.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

☑ Automatically detect settings
□ Use automatic configuration script

Address

Proxy server

☑ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: 72.37.244.115 Port: 8080 [Advanced]

□ Bypass proxy server for local addresses

[OK] [Cancel]

Try browsing to a website now that you are bypassing the ISR. If you are able to browse properly, the problem is most likely with the ISR G2. Check your configurations and routing. If you are unable to browse, the problem is most likely with the CWS tower, and you will have to contact your CWS account representative.

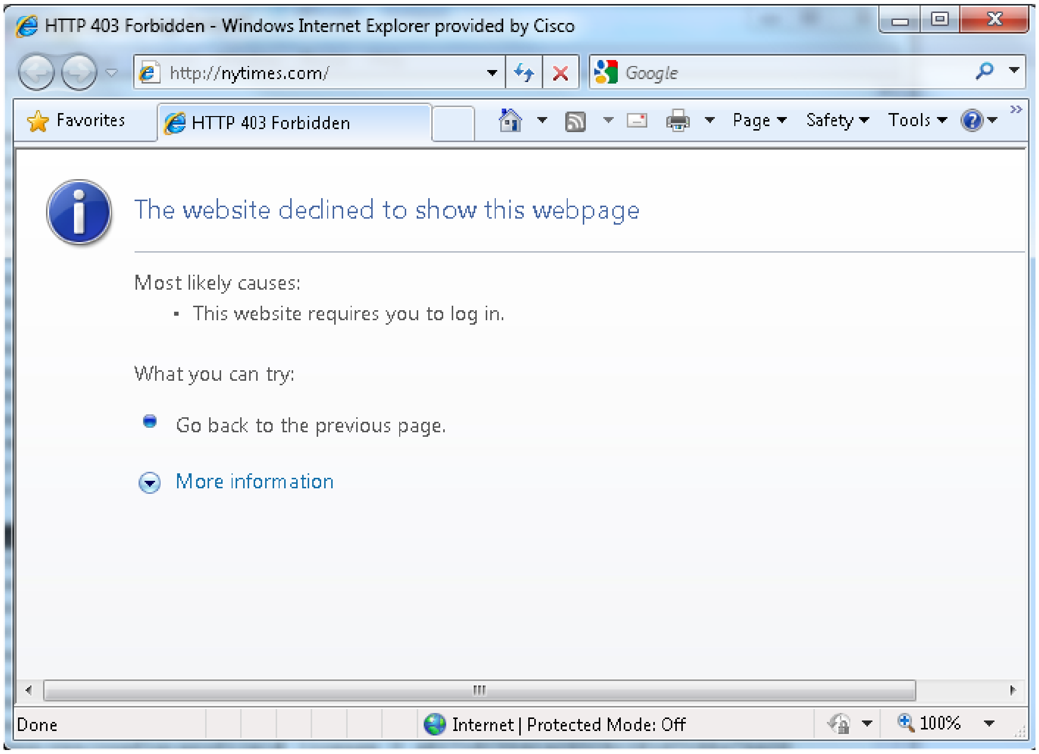
Note: If some users are not able to browse the web but others are able to browse without issues, check whether the users whose pages are not loading are using a different proxy server instead of going through CWS.

Next Steps

- If you are able to browse after configuring a proxy on your browser, the issue resides with the ISR G2. If you need support, open a case with Cisco TAC.
- If you are unable to browse after configuring a proxy on your browser, the issue resides with the CWS tower. If you need support, open a case with Cisco CWS.

License Issues

If you have an invalid CWS license, the output of the **show content-scan summary** command may still show **(Down)** for connections to the tower. However, you will get a “403 Forbidden” error message similar to the one below when browsing.



HTTP 403 Forbidden - Windows Internet Explorer provided by Cisco

http://nytimes.com/

The website declined to show this webpage

Most likely causes:

- This website requires you to log in.

What you can try:

- Go back to the previous page.

More information

Done

Internet | Protected Mode: Off

Next Steps

- Verify that you entered the correct license key information on the ISR G2 with the key provided on the CWS portal.

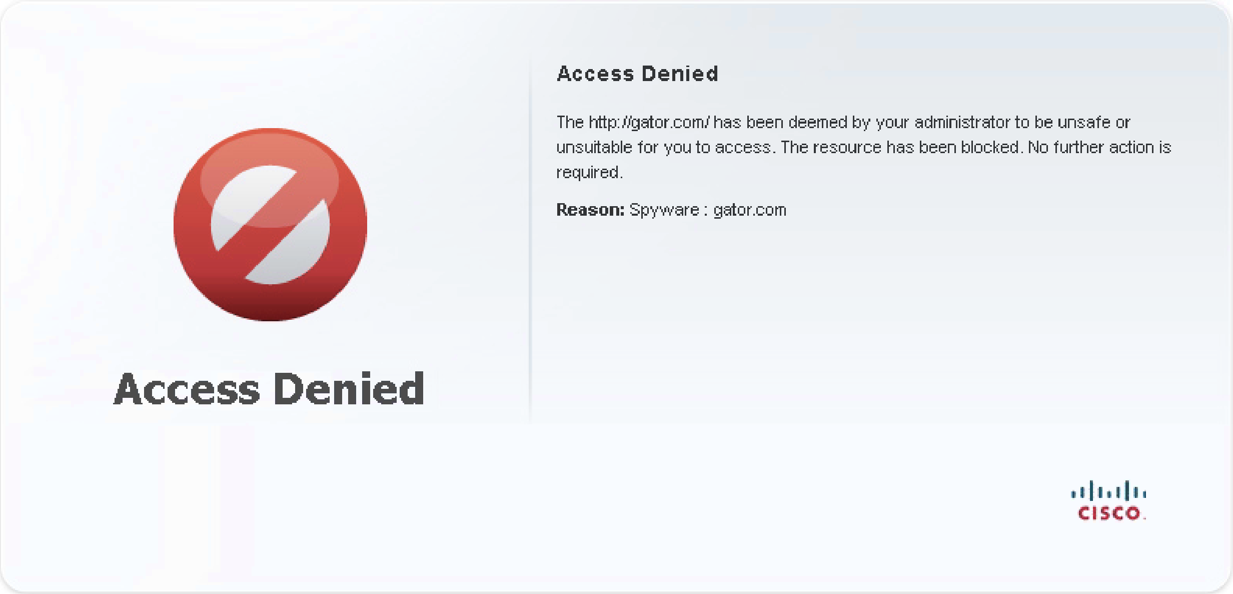
```
parameter-map type content-scan global
 server scansafe primary name proxy197.scansafe.net port http 8080 https 8080
 server scansafe secondary name proxy137.scansafe.net port http 8080 https 8080
!! Make sure the license key on the router is correct
 license 0 AEXXXXXXXXXXXXXXXXXXXXXXXXXXXXXAA39
source interface FastEthernet4
 timeout server 30
 user-group ciscogroup username ciscouser
 server scansafe on-failure block-all
```

- You can also generate and send a new key from CWS in case your key was misconfigured. Details on how to generate and send a key can be found in the ScanCenter Administrator Guide.
- If you are unable to obtain a working license or key, contact Cisco CWS.

CWS Functionality

This section examines other situations in which users are unable to access websites. In this section, we assume that the ISR G2 has connectivity to the CWS tower.

Remember that users will get a warning message from CWS like the one below if they are trying to access a blocked site. This message is part of the CWS functionality.



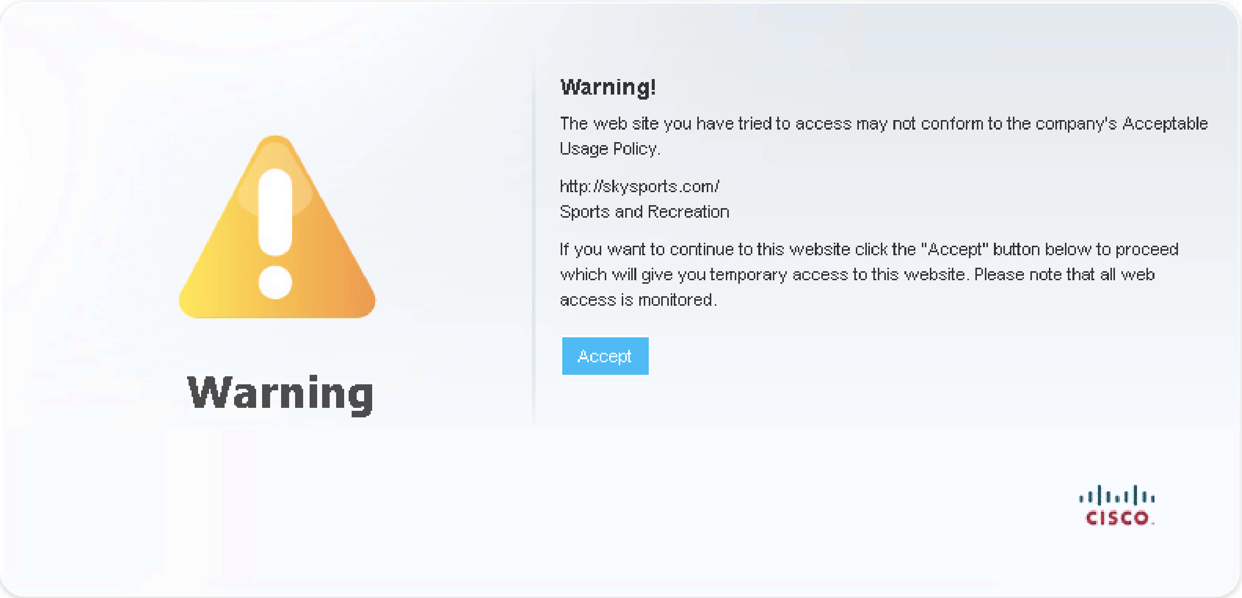
Access Denied

Access Denied

The http://gator.com/ has been deemed by your administrator to be unsafe or unsuitable for you to access. The resource has been blocked. No further action is required.

Reason: Spyware : gator.com

The CWS warning message below is different. By clicking Accept, a user can continue to the site.



Warning!

The web site you have tried to access may not conform to the company's Acceptable Usage Policy.

http://skysports.com/
Sports and Recreation

If you want to continue to this website click the "Accept" button below to proceed which will give you temporary access to this website. Please note that all web access is monitored.

However, if users are reporting that webpages are not loading at all (for example, all they see is a blank page), check for the errors described below.

Mismatched Time Zones

Because CWS uses time-based policies, users will not be able to access websites if the time zone on the ISR G2 does not match the time zone on the CWS tower.

Next Steps

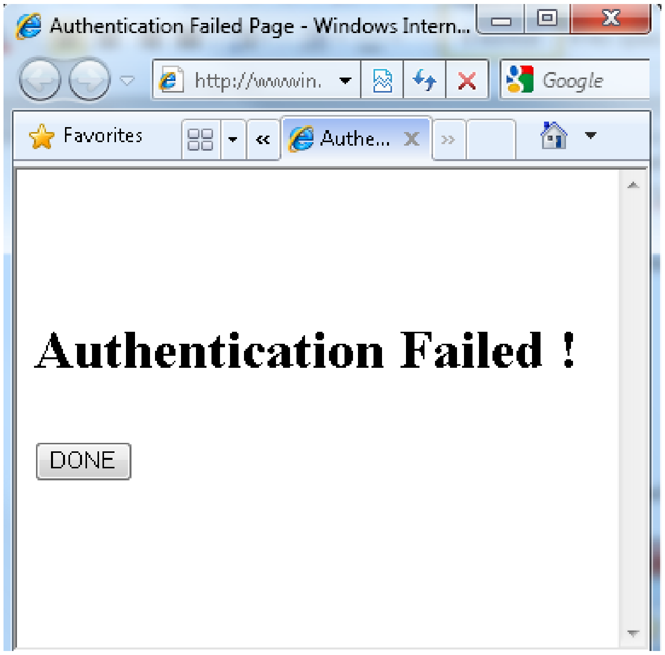
- The simplest way to solve this issue is to configure the ISR G2 to use an NTP server:

  ```
  ntp server 10.0.0.1
  ```

User Authentication Failures

Authentication methods and CWS are two independent features, and customers must use them together to configure precise policies. However, the tips described below can help determine whether customers have encountered an authentication issue or CWS is not functioning as expected.

If users are experiencing authentication failures, they will see an “Authentication Failed” message similar to the one shown below if they are using Web Authentication Proxy.



Authentication Failed !

When using NTLM (active or passive) or HTTP Basic authentication, users are prompted again for their credentials if authentication fails, until the maximum number of login attempts is reached. Once that number is reached, users are moved to a service-denied state until the configurable watch-list timer expires. The default watch-list timer is 30 minutes, after which user can try to authenticate their credentials again.

To view the status of a user, the administrator can enter the **show ip admission cache** command in the router console:

```
router#show ip admission cache
Authentication Proxy Cache
 Client Name cisco, Client IP 10.10.10.4, Port 59400, timeout 1440, Time
Remaining 1440, state ESTAB
```

A user who is in the service-denied state after making too many incorrect login attempts will have service_denied as the state status:

```
router#show ip admission cache
Authentication Proxy Cache
 Client Name guest, Client IP 10.10.10.4, Port 59527, timeout 1440, Time
Remaining 2, state SERVICE_DENIED
```

An administrator can clear the watch-list entry manually by issuing the **clear ip admission watch-list [* | ip address]** to allow the user to reauthenticate.

Note: Firefox and Internet Explorer typically cache credentials for NTLM, and users may not be prompted for credentials after they have been cached.

Both these cases are authentication issues and not CWS issues. The authentication issue should be resolved before further debugging with CWS.

Next Steps

- To check whether a user is being properly authenticated with the authentication, authorization, and accounting (AAA) server, issue the command

test aaa group <AAA server group name> <username> <password> new-code

You should see the message **User successfully authenticated** if authentication passes.

```
router#test aaa group cisco-aaa user1 cisco123 new-code
Trying to authenticate with Servergroup cisco-aaa
User successfully authenticated
```

An incorrect username and password combination will generate a **User rejected** message.

```
router#test aaa group it-aaa user1 cisco123 new
Trying to authenticate with Servergroup it-aaa
router#User rejected
```

A misconfigured AAA server will generate a **server is not reachable** message.

```
router#test aaa group it-aaa user1 cisco123 new
Trying to authenticate with Servergroup it-aaa
router#AAA server is not reachable
```

Other helpful debugging commands for authentication failures include the following:

debug ldap all	Debug LDAP events, errors, legacy, and packets
debug ip admission detail	Debug IP admission API events
debug aaa authentication	Debug AAA authentication events
debug aaa authorization	Debug AAA authorization events

- For more detailed information on authentication, refer to the Cisco IOS® Security Configuration Guide for Authentication, Authorization, and Accounting.
- To contact support, open a case with Cisco TAC.

Session Flows

Taking a closer look at session flows can help determine whether CWS is redirecting traffic properly. To see the total number of redirected sessions as well as white-listed sessions (which bypass the CWS Connector), use the **show content-scan statistics** command.

```
router#show content-scan statistics
Current HTTP sessions: 49
Current HTTPS sessions: 2
Total HTTP sessions: 1486
Total HTTPS sessions: 406
White-listed sessions: 0
Time of last reset: never
-----------------------------------
Details:
Max Concurrent Active Sessions: 55
```

```
Connection Rate in last minute:
    Redirected
        HTTP: 64
        HTTPS: 2
    White-listed
        IP-Based: 0
        User/User-group: 0
        Header-Based: 0
Max Connection Rate per minute:
    Redirected
        HTTP: 154
        HTTPS: 76
    White-listed
        IP-Based: 0
        User/User-group: 0
        Header-Based: 0
```

The highlighted text in the above example shows that CWS is indeed redirecting traffic to the tower.

Issuing the **show content-scan statistics memory-usage** command will show the number of CWS entries, connections, and HTTP(S) requests:

```
router#show content-scan statistics memory-usage
Chunk Name                         Size(bytes)   Chunks in use
Content-Scan entry                        5048               0
User-Group                                  84               0
HTTP Request                              7520               0
HTTPS Request                             7020               0
HTTPS SSL                                 1520               0
Buffer Packet                               24               0
```

Finally, issuing the **show content-scan statistics failures** command will provide the number of failures, if there are any.

```
router#show content-scan statistics failures
Reset during proxy Mode:                     0
HTTPS reconnect failures:                    0
Buffer enqueue failures:                     0
Buffer length exceeded:                      0
Particle coalesce failures:                  0
L4F failures:                                0
Lookup failures:                             0
Memory failures:                             0
Tower unreachable:                           0
Resets sent:                                 0
Interrupt reconnect lock failures:           0
Process reconnect lock failures:             0
Duplicate Content Scan entries:              0
```

```
Mismatch CS Entry and L4F App ctx:           0
L4F APP Context NULL                         0
Content Scan Entry with NULL FD              0
```

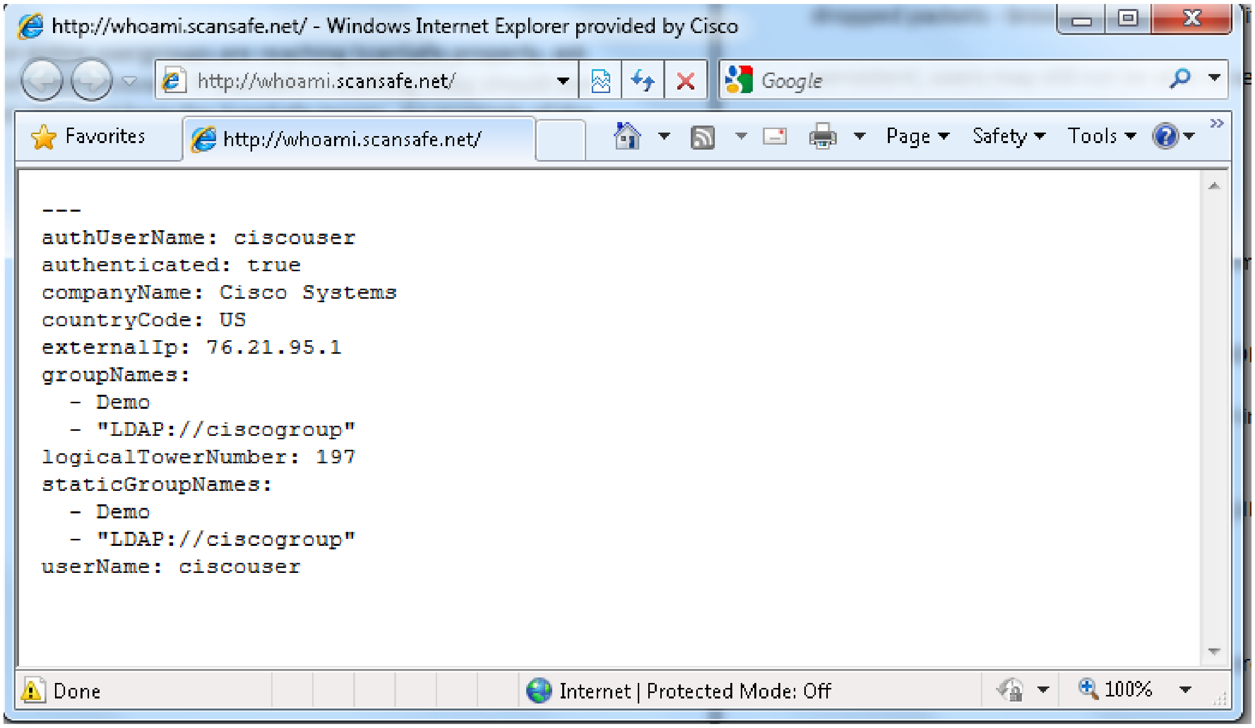
To see individual active sessions that are being redirected by CWS, use the **show content-scan session active** command.

Note: The **show content-scan session active** command may result in numerous entries if many users are connected and actively browsing. It may be beneficial to filter results by username/usergroup or IP address. URIs are only shown for HTTP requests, not HTTPS requests.

```
router#show content-scan session active
Protocol      Source        Destination     Bytes             Time
HTTPS 10.32.251.117:52775 74.125.224.117:443 (12433:9302) 00:05:08
        URI:
        Username/usergroup(s): ciscouser/ ciscogroup
HTTPS 10.32.251.117:52788 74.125.224.54:443 (6577:2633) 00:01:08
        URI:
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52789 98.137.88.35:80 (999:59478) 00:00:39
        URI: l1.yimg.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52790 157.166.226.25:80 (8896:26025) 00:00:12
        URI: www.cnn.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52791 157.166.226.25:80 (5904:6352) 00:00:11
        URI: www.cnn.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52792 63.80.138.66:80 (907:635) 00:00:11
        URI: z.cdn.turner.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52795 204.2.133.120:80 (413:317) 00:00:11
        URI: content.dl-rms.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52797 209.244.156.19:80 (2926:2124) 00:00:11
        URI: ad.insightexpressai.com
        Username/usergroup(s): ciscouser/ ciscogroup
HTTP 10.32.251.117:52798 63.80.138.35:80 (1546:269) 00:00:11
        URI: icompass.insightexpressai.com
        Username/usergroup(s): ciscouser/ ciscogroup
```

Next Steps

- As a final check to determine whether individual users or entire usergroups are going through CWS properly, ask the user to go to **http://whoami.scansafe.net/** on their browser. If CWS is working, they should see an output with details of their usergroup account obtained from the CWS tower. An example of the output is provided below.


http://whoami.scansafe.net/ - Windows Internet Explorer provided by Cisco
http://whoami.scansafe.net/
Google
Favorites
http://whoami.scansafe.net/
Page
Safety
Tools
Done
Internet | Protected Mode: Off
100%

```
---
authUserName: ciscouser
authenticated: true
companyName: Cisco Systems
countryCode: US
externalIp: 76.21.95.1
groupNames:
  - Demo
  - "LDAP://ciscogroup"
logicalTowerNumber: 197
staticGroupNames:
  - Demo
  - "LDAP://ciscogroup"
userName: ciscouser
```

- If redirection to CWS is happening, and users are still unable to load webpages, debugging should be performed on the CWS tower side, as the connector on the ISR G2 is functioning properly. To contact support, open a case with Cisco CWS.
- If redirection to CWS is *not* happening, debugging should be performed on the ISR G2 side. To contact support, open a case with Cisco TAC.

User Experience

This section explores situations in which users complain of slow-loading pages, pages that hang, and other poor experiences. Again, we assume that connectivity to the CWS tower is established and that CWS is properly redirecting traffic.

User experience complaints may be the most difficult to diagnose and must often be done on a case-by-case basis. Remember that there may be a slight delay when CWS is operational as packets are redirected to the CWS tower first. This delay is normal. For users that complain about excessive delays before the browsers load, you may have to perform a packet capture of the session to see where the congestion lies.

On extremely rare occasions, the ISR G2 may drop packets because it has hit the maximum number of sessions. In this case, users may not see their webpages load for a few moments. Typically, the browser will retransmit the packets, but if the sessions are persistent, users may experience a slight delay in page loads before retransmission occurs. Once the packets are retransmitted, users should be able to view their pages properly.

A syslog message will warn administrators when the maximum number of sessions is reached:

```
*May 2 09:19:06.877: %L4F-6-L4F_FLOW_LIMIT_EXCEED: L4F flows fd limit
exceeded:32678.
```

Alternatively, you can use the **show l4f statistics** command to manually check the Layer 4 forwarding database and packet information.

```
router#show l4f statistics
L4F Global Statistics               Process     Interrupt
Client register                          13             0
Client deregister                        10             0
Client lookup failure                   158            12
Policy check accepted                     0          2075
Policy check rejected                  2816            21
Flows created                             0          2075
Flow creation failed                      0             0
Flows destroyed                        2075             0
Flows forced to bypass                    0             0
Flow lookup failed                    27989         55801
Flow cleanup scans                      299             0
Flows delayed for reinjection             0             0
Packet interception FORWARD          122045         70567
Packet interception PROXIED              56          1941
Packet interception BYPASS            28006         53726
Packet interception ABORT                 0             0
Packet interception DROP                  7             0
Packet interception CONSUME            3686          2708
Packet interception PUNT                  0          8026
Packet interception UNKNOWN               0             0
Packet interception forced punt           0             0
Spoofing to proxying failures             0             0
Spoofing to proxying success             56          1954
Spoofing to proxying timeouts            34             0
Spoofing to proxying SACK                56          1954
Spoofing to proxying Timestamp            0             0
Spoofing to proxying Window Scal          0             3
Unproxy connections                     703          1288
Unproxy connection rejected               0             0
Unproxy completed                      1991             0
Read notify called                      121          2718
Read notify aborted                       0             0
Read notify punt                          0            10
Read notify ok                          121          2718
Read buffer                              10            10
Read packet                             188          5416
Write notify called                     739             0
Write notify aborted                      0             0
Write notify punt                         0             0
Write notify ok                         739             0
Write buffer                           1036          3800
Write packet                              0             0
APIs returning EBUSY                      0             0
Connect notify called                     0             0
Connect notify ok                         0             0
Connect notify error                      0             0
Reconnect called                          0             0
Close notify called                    2075             0
Unproxy complete called                1991             0
Shutdown called                          32             0
Close called                              0             0
Abort called                              6             0
Spoofing mode packets                  4249          1954
Proxying mode packets                  3426          3903
Unproxying mode packets                2414             0
Unproxied mode packets                  207         70567
Packet reinject state alloc fail          0           152
Packet buffer alloc failed                0             0
Packet reinjection                     1830          2974
Packet reinjection punts                  0             0
Packet reinjection errors                 0             0
Packet reinjection other                  3             0
Packets delayed for reinjection           0             0
Packets drained from delay q              0             0
Packets freed from delay q                0             0
```

Next Steps

- To determine where the root cause of a poor user experience lies, find out whether there have been any issues with latency on the CWS tower side. Your Cisco sales contact should be able to help you make this inquiry.
- If no latency issues are reported on the CWS tower side, the root cause may lie in the ISR G2 or the network. To contact support, open a case with Cisco TAC.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

Co7-732660-00 09/14