Cisco Integrated Services Router Generation 2 with Cisco Cloud Web Security

Solution Guide

Contents

Overview

The Cisco® Integrated Services Router (ISR) Generation 2 (G2) family delivers numerous security services, including firewall, intrusion prevention, and VPN. These security capabilities have been extended with Cisco Cloud Web Security for a web security and web filtering solution that requires no additional hardware or client software.

The Cisco ISR G2 with Cloud Web Security solution enables branch offices to intelligently redirect web traffic to the cloud to enforce granular security and acceptable use policies over user web traffic. With this solution, you can deploy market-leading web security quickly and easily to protect branch office users from web-based threats such as viruses, while saving bandwidth, money, and resources.

You can use the Cisco ISR with Cisco Cloud Web Security to:

- Enforce granular security and acceptable use policy for branch office users without using on-premises hardware or backhauling all branch office traffic to the headquarters
- Provide zero-day threat protection driven by Outbreak Intelligence, which uses dynamic reputation- and behavior-based analysis

Cisco Cloud Web Security is compatible with Cisco ISR G2 products (see the list of supported platforms later in this document). After configuring the Cisco ISR G2 with Cloud Web Security, you can use the Cloud Web Security portal to create, edit, and manage Cloud Web Security accounts and policies.

Benefits of Using the ISR G2 with Cisco Cloud Web Security

Using the Cisco ISR G2 with Cisco Cloud Web Security has the following benefits:

- **Lower total cost of ownership:** Cisco ISR G2 with Cloud Web Security helps you avoid costs associated with the deployment and maintenance of on-premises software and hardware.
- **Leading security and peace of mind:** Real-time cloud-based scanning blocks malware and inappropriate content before it reaches the network.
- **Scalability and availability:** The global network processes high volumes of web content at high speeds, everywhere, for a truly global solution that is always available.
- **Integration with other Cisco security products:** Cisco ISR G2 with Cloud Web Security integrates with Cisco AnyConnect® to offer a web security solution for users both on and off the network.
- **Consistent, unified policy:** Acceptable use policy (AUP) can be applied to all users regardless of location, simplifying management.
- **Predictable operational expenses:** Clients can plan capacity and budget.
- **Centralized management and reporting with the Cloud Web Security portal:** The Cisco Cloud Web Security portal is a web-based interface that integrates all management and reporting capabilities. Global web security policies can be created and enforced across the organization, even at the group or user level, and any changes to these policies are applied in real time. The Cloud Web Security portal includes real-time reporting.

Note: This document focuses on configuring the Cisco ISR G2. For more information on configuring and using the Cloud Web Security portal, refer to the Cisco Cloud Web Security Portal Administrator Guide.

Licensing

The Cloud Web Security feature on the Cisco ISR G2 is available with the Security SECK9 license bundle. For more information on configuring the Security SECK9 license bundle, refer to the Cisco ISR G2 Licensing and Packaging white paper.

Supported Platforms and Architectures

Table 1 lists the Cisco ISR G2 platforms compatible with Cloud Web Security.

Table 1. Supported Platforms

Product	Supported Platforms
Cisco 800 Series ISRs	Cisco 819, 860VAE, 880VA, 881, 881W, 887V, 888E, 888EA, 888, 888W, 891, 891W, 892, 892F, 892FW, 892W
Cisco 1900 Series ISRs	Cisco 1905, 1921, 1941, 1941W
Cisco 2900 Series ISRs	Cisco 2901, 2911, 2921, 2951
Cisco 3900 Series ISRs	Cisco 3925, 3925E, 3945, 3945E

The Cisco ISR G2 and Cisco Cloud Web Security Design Guide provides details of supported architectures and best practices.

Understanding How the ISR G2 Works with Cisco Cloud Web Security

When Cisco Cloud Web Security is enabled and the Cisco ISR G2 is configured to redirect web traffic to the Cloud Web Security server, the ISR transparently redirects HTTP and HTTPS traffic to the Cloud Web Security proxy servers based on the destination IP address and port number. The Cloud Web Security proxy servers scan the content and either allow or block the traffic based on the configured policies, to enforce acceptable use and protect clients from malware.

The Cisco ISR G2 authenticates and identifies users who make web traffic requests using the configured authentication and authorization methods. The router encrypts and includes the user information (username and user groups) in the traffic that it redirects to the Cloud Web Security server. The Cloud Web Security server uses the user credentials to determine the web policies to apply to users, and for user-based reporting.

You can configure the Cisco ISR in such a way that some web traffic goes directly to the originally requested web server and does not get scanned by Cloud Web Security. For more information, see the section Bypassing Cisco Cloud Web Security Scanning.

You can configure a primary and a backup Cloud Web Security proxy server. The Cisco ISR polls each server regularly to check for its availability. You can change this polling interval using the command-line interface (CLI).

Communication Between the Cisco ISR G2, Cisco Cloud Web Security, and Clients

Clients are any devices that connect to a Cisco ISR, either directly or indirectly. When a client sends an HTTP or HTTPS request, the Cisco ISR receives it and forwards it to the Cloud Web Security proxy server. If authentication is configured, the Cisco ISR first authenticates the user and then retrieves the group name from the authentication server. The router maintains an IP address-to-user name mapping for future reference. After identifying the user (if applicable), the Cisco ISR determines whether to send the HTTP or HTTPS client request to the Cloud Web Security server by checking the Cisco IOS® Firewall Port to Application Mapping (PAM) and whitelist database.

For information about PAM, see the Configuring Port to Application Mapping chapter in the *Cisco IOS Security Configuration Guide: Context-Based Access Control Firewall*.

For more information about the whitelist database, see the Bypassing Cisco Cloud Web Security Scanning section in this document.

When the Cisco ISR sends a client request to Cloud Web Security servers, it acts as an intermediary between the client and Cloud Web Security servers by creating a separate connection with the Cloud Web Security proxy server. When the Cisco ISR communicates with Cloud Web Security, the router changes the destination IP address and destination port number of the client request. It adds Cloud Web Security-specific HTTP headers, which include information about the username and user group, and sends the modified request to Cloud Web Security servers. For more information about the headers, see the next section, Cisco Cloud Web Security Headers.

When the Cloud Web Security server receives an HTTP or HTTPS request from a Cisco ISR, it uses the information and user credentials in the Cloud Web Security HTTP headers to apply appropriate policies to the user. When the request returns from the server to the client, the source address is changed. After applying the configured policies, Cloud Web Security either allows, blocks, or presents a warning message before allowing a client request:

- **Allow:** When Cloud Web Security allows a client request, it contacts the originally requested server and retrieves data. It forwards the server response to the Cisco ISR, which then forwards the response to the client. The Cisco ISR changes the source and destination IP addresses and port numbers in the response as appropriate.
- **Block:** When Cloud Web Security blocks a client request, it sends an HTTP 302 “Moved Temporarily” response that redirects the client application to a web page hosted by Cloud Web Security. This page notifies the user that access has been blocked. The Cisco ISR forwards the 302 response to the client while changing the source and destination IP addresses and port numbers.

Note: Administrators can customize the block page using the Cloud Web Security portal.

- **Warn:** In some instances, the administrator may not completely block access to particular sites but will need to let customers know that the site they are trying to access may not fully comply with company policies. In this case, Cloud Web Security can first present a page hosted by Cloud Web Security with a warning message and an “accept” button. If customers click the accept button, they are allowed access to the site.

Note: Administrators can customize the warning page using the Cloud Web Security portal.

You can choose how the Cisco ISR handles web traffic when it cannot reach either the primary or backup Cloud Web Security proxy server. The router can block or allow all web traffic. By default, it blocks web traffic.

Note: The Cisco ISR G2 routers do not have any native ability to detect apps on mobile devices, even web-based apps. As a result, traffic from apps launched on mobile devices and tablets may not be blocked or warned as per the configured the Cloud Web Security policies. However, if the content is accessed through a web browser, it will be blocked or warned according to specified policies.

For example, Facebook access may be blocked by the configured Cloud Web Security policies of a company. Employees of this company will not be able to access Facebook through Safari on an Apple iPad; however, they may be able to access Facebook through the Facebook app installed on the Apple iPad.

Cisco Cloud Web Security Headers

When a Cisco ISR G2 router forwards web traffic to Cloud Web Security proxy servers, it includes additional HTTP headers in each HTTP and HTTPS request. Cloud Web Security uses these headers to obtain information about

the user who made the client request, as well as information about the Cisco ISR G2 router that sent the request. For security purposes, the information in the headers is encrypted and then hexadecimal-encoded.

Cisco Cloud Web Security headers provide both asymmetric cryptography and symmetric cryptography by using industry-standard algorithms. Asymmetric encryption is done by using the RSA/ECB/PKCS1Padding algorithm, which uses key pairs of 512 bits. Symmetric encryption is done by using the triple “DESede” algorithm with a randomly generated triple Data Encryption Standard (DES) key of 168 bits.

The Cisco ISR adds the following Cloud Web Security HTTP headers:

- **X-ScanSafe:** This header contains a session key that is encrypted using a Cloud Web Security public key (embedded in the ISR operating system).
- **X-ScanSafe-Data:** This header contains the data Cloud Web Security needs. It is encrypted with the session key from the X-CWS header. For example, the headers in a message might look like the following:
- **X-ScanSafe:** 35A9C7655CF259C175259A9B980A8DFBF5AC934720BE9374D344F7E584780ECDB9236FF90DF562A79DC4C75 4C3782E7C3D38C76566F0377D5689E25BD62FC5F
- **X-ScanSafe-Data:** 8D57AEE5D76432ACAB184AA807D94A7392986FA0D3ED9BEB

Bypassing Cisco Cloud Web Security Scanning

You can configure the Cisco ISR G2 in such a way that only approved web traffic is not redirected to Cloud Web Security for scanning. When Cloud Web Security scanning is bypassed, the Cisco ISR G2 retrieves the content directly from the originally requested web server without contacting Cloud Web Security. When the Cisco ISR G2 receives a response from the web server, it sends the data directly to the client. This is also called “whitelisting” of traffic.

You can bypass scanning based on the following client web traffic properties:

- **IP address:** Bypass the scanning of web traffic that matches a numbered or named access control list (ACL) configured in the global parameter map on the Cisco ISR G2. You can bypass scanning for traffic to trusted sites, such as intranet servers.
- **HTTP header fields:** Bypass the scanning of web traffic that matches an HTTP header field configured in a global parameter map on the Cisco ISR G2. You can configure a match based on Host or User-Agent header fields. You can configure this type of scanning bypass for particular user agents that do not function properly when scanned, or for traffic that is intended for trusted hosts, such as third-party partners.

Note: When HTTP header-based whitelisting is enabled, the Cisco ISR G2 automatically disables/removes TCP options such as windows scaling and timestamps.

- **Username or user group:** Bypass the scanning of web traffic that matches a username or the user group a user belongs to. You can bypass scanning for a subset of trusted users.

Use the content-scan whitelisting command and then the whitelist command to create a whitelist database for traffic that can bypass scanning.

For more information, see the Configuring Whitelisting section in this document.

Working with Multiple ISRs

A typical branch office uses one Cisco ISR G2 to route network traffic to headquarters and to redirect web traffic to Cloud Web Security for security scanning. However, your organization might have multiple branch offices with one Cisco ISR G2 in each office.

These Cisco ISR G2 routers may force users to authenticate before granting them network access. When the Cisco ISR G2 enforces authentication, in the redirected web traffic, the ISR G2 sends user group information, received from an authentication server, about the user making the web request. When authentication is not enforced, user group information is not sent from the authentication server. You can configure a default user group name for all web traffic using the user-group command when you configure the web security feature on the ISR.

Each Cisco ISR must be configured with a license (authentication key) in the Cloud Web Security portal. The Cloud Web Security portal supports company and group authentication keys.

If your network has multiple Cisco ISRs and branches, you can choose the type of Cloud Web Security authentication key you need to create and use when you configure each Cisco ISR. Creating the authentication key depends on whether or not the Cisco ISR enforces authentication:

- **No authentication on the Cisco ISR G2:** Cloud Web Security applies the same web policies to all traffic originating from a single ISR. To apply different web policies for traffic from different ISRs, use and generate a group key in the Cloud Web Security portal for each ISR. Configure a different group key as the license in each ISR router configuration. To apply the same web policies for traffic from all ISRs, use and generate a company key in the Cloud Web Security portal, and configure it as the license in each ISR router configuration. A company key is a key used by your entire organization.
- **Authentication on the Cisco ISR G2:** When the ISR enforces authentication, it sends user-group information from an authentication server in the redirected web traffic. Cloud Web Security helps you apply different web policies for different user groups. You can generate a company key in the Cloud Web Security portal and configure it as the license in each ISR configuration. You can choose to apply the same or different Cloud Web Security policies to different user groups.

For more information on generating Cloud Web Security authentication keys, see the Creating a Cisco Cloud Web Security Authentication Key section in this document.

Configuring Cisco Cloud Web Security on the ISR G2

To use the Cisco ISR G2 with Cisco Cloud Web Security, you must configure the following:

- Cisco ISR G2 that uses Cisco IOS Release 15.3(3)M or later.

Note: The recommended image is Cisco IOS Release 15.3(3)M or later; however, Cloud Web Security works with Cisco IOS Releases 15.2(1)T1 and later releases.
For a list of supported platforms, see the Supported Platforms and Architectures section in this document.

- Cisco Cloud Web Security portal. For more information, see the Configuring the Cisco Cloud Web Security Portal section in this document.
- Before you can enable Cloud Web Security on the Cisco ISR, create a company or group key in the Cloud Web Security portal. For more information, see the Creating a Cisco Web Security Authentication Key section in this document.

Configuring Cisco Cloud Web Security Features

Use the CLIs listed in Table 2 to configure parameters for Cloud Web Security.

Table 2. Configuring Parameters for Cloud Web Security

Command	Description
`parameter-map type content-scan global`	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.
`[no] server scansafe {primary | secondary} ipv4 <ip-address> port http <port-no> https <port-no>`	Configures the server name or IP address of the primary and/or secondary Cloud Web Security proxy servers, as well as ports to use for redirecting HTTP and HTTPS requests. Cloud Web Security uses port 8080 for both HTTP and HTTPS traffic. **Note:** Only the primary Cloud Web Security server is mandatory, although it is recommended to configure the secondary server for backup/failover purposes. Only one port configuration is mandatory; traffic from ports that are not configured are whitelisted. For example, if the HTTPS port is not configured, all HTTPS traffic is whitelisted.
`[no] timeout {server <5- 43200> |session inactivity <5- 3600>}`	"Timeout server" configures the amount of time the ISR waits before polling the Cloud Web Security proxy server to check its availability. Default timeout is 60 seconds. The ISR checks the primary server first, and if it fails, it uses the secondary server as the active Cloud Web Security proxy server. The ISR automatically falls back to the primary server as long as it is successfully active for three consecutive timeout periods. "Timeout session inactivity" configures the amount of time the ISR waits before closing an inactive session. Default timeout value is 1800 seconds.
`server scansafe on-failure {allow-all | block-all}`	Determines how to handle client traffic when the ISR cannot reach either of the configured Cloud Web Security proxy servers. You can either block or allow all client web traffic. The default is block.
`[no] license {0 | 7} <16 byte Hex key>`	Configures the license key that the ISR sends to the Cloud Web Security proxy servers to indicate the organization from which the request comes. The license is a 16-byte hexadecimal key. Use one of the following values for the prefix: • 0: This value indicates that the license is unencrypted. (32 characters) **Note:** If "service password-encryption" is enabled, the key will be encrypted afterward in accordance with option 7 below. • 7: This value indicates that the license is encrypted. (66 characters) The license key you specify here comes from the Cloud Web Security portal. In the portal, you can create either a company or a group key. For more information on how to do this, see the Creating a Cisco Cloud Web Security Authentication Key section in this document.
`[no] source {ipv4 <ip-address> | interface <interface>}`	Source IP or tower interface used to poll the tower for diagnostics and event updates. **Note:** The source interface or IP address should be routable to the Cloud Web Security tower. The interface can be either logical or physical, as long as it can reach the Cloud Web Security tower properly. When there are dual WAN links from two different service providers, it is recommended to configure a loopback IP address or interface instead of using one of the WAN links. If the IP address is unknown, the interface used to obtain the Dynamic Host Configuration Protocol (DHCP) address should be used.

Command	Description
`[no] user-group {group name <groupname> [username <username>] | exclude <groupname> | include <groupname>}`	This command is optional. You can use this subcommand to manage user and group information the ISR sends to Cloud Web Security in the HTTP headers for redirected client requests. **Groupname:** You can enter a default group name that applies to all users when there is no specific group name for a client request from authentication. The group name is case-sensitive. The ISR prepends the group name with "LDAP://" in the HTTP header when it redirects web traffic to Cloud Web Security. Any group name entered here must match a configured group name in the Cloud Web Security portal. **Note:** User group information from authentication methods and then from the default user group configured directly under the interface take precedence over this parameter-map user group. If no user group information is found from authentication, the interface default user group information will be taken. If there is no interface default user group, the ISR will forward the parameter-map default user group to the Cloud Web Security tower. **Include and exclude:** By default, the ISR lists all authentication user groups to which a user belongs when it redirects a client request to Cloud Web Security. However, you can use the *include* and exclude options to filter which user groups the ISR sends to Cloud Web Security. Use the exclude option to send all authentication user groups except for the ones specified with the exclude option, and use the include option to create a subset of users inside the available user group list. If the user group name configured with the include option is not part of the existing user group list, no user group information will be sent to the Cloud Web Security tower.
`[no] logging`	Enables IOS syslogs for this feature.

For example, you might use the following configuration:

```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.244.147 port http 8080 https 8080
 server scansafe secondary ipv4 80.254.145.147 port http 8080 https 8080
 license 0 AA01234567890123456789012345678 9

 source interface GigabitEthernet0/0
 timeout server 30

 user-group ciscogroup username ciscouser

 server scansafe on-failure allow-all
```

Another variation of the configuration could be:

```
parameter-map type content-scan global
 server scansafe primary name proxy123.scansafe.net port http 8080
 server scansafe secondary name proxy456.scansafe.net port http 8080
 license 0 AA01234567890123456789012345678 9

 source interface GigabitEthernet0/0
 timeout server 30

 user-group ciscogroup username ciscouser
```

```
server scansafe on-failure block-all
```

In the second example, the Cloud Web Security tower name is used instead of the tower IP address.

Note: Use the tower IP address over the name for faster lookups.

The HTTPS port is also not specified, which means that all HTTPS traffic will be whitelisted. Finally, the default action in the example is to block all traffic if Cloud Web Security towers are not reachable. This means that if both the primary and secondary Cloud Web Security towers are unreachable, users will not be able to access the Internet.

At this point, Cloud Web Security has been configured but not enabled on the ISR G2.

Enabling Cisco Cloud Web Security on the ISR G2

Enable content scanning on the ISR on the egress interface. The content-scanning process is the Cisco IOS process that redirects client web traffic to Cisco Cloud Web Security.

Do this by adding the following configuration to the interface CLI command:

```
content-scan out
```

For example, you might use the following configuration for an egress interface:

```
interface GigabitEthernet0/0
 ip address 10.0.0.1 255.255.255.0
 ip virtual-reassembly in
 ip virtual-reassembly out
 content-scan out
 duplex auto speed auto
```

Note: If you enable content scanning on an interface with Cisco Wide Area Application Services (WAAS), WAAS Express, or Multiprotocol Label Switching (MPLS), verify that Cisco Cloud Web Security does not apply to the same network traffic as either WAAS or MPLS.

Configuring Whitelisting

You can configure the ISR G2 to bypass Cloud Web Security scanning for approved web traffic.

To bypass scanning of traffic, use the content-scan whitelisting command (a global command) and the whitelist subcommand. Use the following syntax for the whitelist subcommand:

```
content-scan whitelisting
 [no] whitelist
{acl {<acl#> | name <acl name>} |
header {host regex <host regex name> |
user-agent regex <user-agent regex name>}}
```

Use the subcommands in Table 3 to configure the whitelist subcommand.

Table 3. Options for Configuring the Whitelist Subcommand

Command	Description
`acl {<acl number> | name>`	The IP addresses used will be the pre-Network Address Translation (NAT) IP addresses for matching the ACL.
`header {user-agent | host regex <pmap>}`	Specifies the whitelisting attribute on the HTTP header that matches the configured regular expression.

For example, you might use the following configuration:

```
content-scan whitelisting
 whitelist header host regex whitelistedPatterns
 whitelist acl name whitelistedSubnets
 whitelist user regex whitelistedUsers
 whitelist user-group regex whitelistedUserGroups

parameter-map type regex whitelistedPatterns
 pattern cisco[.]com
 pattern google

parameter-map type regex whitelistedUsers
 pattern jchambers123

parameter-map type regex whitelistedUserGroups
 pattern LATAMUser

ip access-list standard whitelistedSubnets
 permit 10.0.0.0 0.0.0.255
```

Whitelisting is conducted in the following order: acl, user, user group, header user-agent, header host.

Note: User, user group, and IP/ACL-based whitelisting is done initially during the TCP SYN. No content-scan sessions are created when a session is whitelisted based on username or user group. For more information about the parameter-map type regex CLI command, see the Cisco IOS Security Command Reference and the Additional Documentation section of this document.

Special Consideration for Whitelisting HTTPS Traffic

By default, Cloud Web Security forwards both HTTP and HTTPS traffic to the Cloud Web Security server. However, you can use the whitelisting feature to bypass HTTPS traffic from Cloud Web Security redirection.

To whitelist HTTPS traffic, first create an ACL that matches the HTTPS traffic, then add this ACL to the Cloud Web Security whitelist:

```
ip access-list extended matchHTTPS
 permit ip any any eq 443

content-scan whitelisting
```

```
 whitelist acl name matchHTTPS
```

Alternatively, you can remove the HTTPS port configuration in the Cloud Web Security parameter map:

```
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.244.147 port http 8080
 server scansafe secondary ipv4 80.254.145.147 port http 8080
```

Configuring a Default User Group

You can configure a default user group on the outbound interface to assign to each client when the ISR cannot determine the credentials of a user. Define a default user group using the following CLI command:

```
interface [interface name]
 [no] user-group default <name>
```

The ISR uses the default user group name here to identify all clients connected to a specific interface on the ISR when it cannot determine the user's credentials. You can define a default user group so that all traffic redirected to the Cloud Web Security proxy servers are assigned a user group to ensure that particular Cloud Web Security policies are applied. For example, you might want to create a default user group for guest users on the wireless network.

Only one user group can be defined per interface.

Note: The order of user groups is as follows: (1) user group information from authentication methods (such as Active Directory group info), (2) interface default user group, (3) parameter-map default user group. If no user group information is found from authentication, the interface default user group information is taken. If there is no interface default user group, the ISR forwards the parameter-map default user group to the Cloud Web Security tower.

Configuring Authentication with Cisco Cloud Web Security

Three types of authentication are supported with Cloud Web Security on the Cisco ISR G2: Windows NT LAN Manager (NTLM), HTTP Basic, and Web authentication. Refer to Table 4 for the authentication types supported on various Cisco IOS releases.

Table 4. Authentication Types Supported on Cisco IOS Releases

Cisco IOS Release	Cloud Web Security Authentication Supported
15.2(1)T1, 15.2(1)T2, 15.2(2)T1	Web and HTTP Basic authentication
15.2(4)M and later	NTLM, HTTP Basic, and Web authentication

The following section provides an overview of the Cisco IOS CLI commands to configure NTLM or HTTP Basic authentication on the ISR G2 to pass user group information to the Cloud Web Security proxy servers.

To configure Web authentication, refer to the Configuring Authentication Proxy chapter in the Security Configuration Guide: Authentication Proxy Configuration Guide.

Configuring NTLM or HTTP Basic Authentication

With NTLM authentication, the ISR tries to retrieve user credentials transparently from the client application without prompting end users for information. If the client application cannot send user credentials transparently, it prompts users to enter credentials. For more information, see the Transparent Authentication with NTLM section in this document.

With HTTP Basic authentication, client applications always prompt users to enter their credentials.

When using NTLM authentication, you can choose two modes, active or passive. By default, active mode is selected for NTLM authentication. To enable passive mode, configure the keyword “passive” in the ip admission CLI command. For example:

```
ip admission name [rule-name] ntlm passive
```

NTLM active causes the ISR to collect both the username and password from the client during the handshake process and verify both against the Active Directory domain controller. When NTLM passive is used, the ISR queries only for the user group and does not verify the password, which also reduces the number of transactions between the ISR and the domain controller.

Use the commands in Table 5 to configure NTLM or HTTP Basic authentication on the ISR G2.

Table 5. Configuring NTLM or HTTP Basic Authentication

Command	Description
`aaa new-model`	Enables authentication commands. **Note:** Once aaa new-model is enabled, it cannot be disabled

`ldap server <server name>`
`ipv4 <ip address>`
`attribute map <map name>`
`bind authenticate root-dn <root-dn attributes>`
`base-dn <base-dn names>`
`authenticate bind-first`
	Defines an LDAP server and its attributes. For more information on configuring the LDAP server, refer to the AAA LDAP Configuration Guide.
	Note: If passive NTLM authentication is used, the root-dn configuration is mandatory.

`ldap attribute-map <map name>`
`map type <ldap attribute type> <aaa attribute type>`
	Configures a dynamic LDAP attribute map.
	Example:
	`ldap attribute-map ldap-map`
	`map type sAMAccountName username`
	For more information on configuring the dynamic LDAP attribute map, refer to the AAA LDAP Configuration Guide.

`aaa group server ldap`	Defines one or more LDAP groups.
`aaa authentication login`	Defines authentication services.
`aaa authorization login`	Defines authorization services.
`ip admission`	Defines IP admission parameters.

Command	Description
`ip admission virtual-ip <ip address> virtual-host <hostname>`	Optional. Required only for transparent authentication with NTLM. Defines proxy URL IP address and host names for clients to be redirected to a virtual proxy for authenticating users. The IP address should not correspond to an existing device on the network and should not have the same IP address as any interface on the ISR G2. The virtual proxy host name is a single-word, nonqualified domain name. An example of a virtual IP and host name combination could be 1.1.1.1 and "webproxy," respectively. Here it is assumed that the client will have the DNS suffix to resolve the virtual host name. If this is not the case, the fully qualified domain name (FQDN) needs to be added for the virtual host name.
`int <interface>` `ip admission <rule name>`	Applies the IP admission rule to the ***internal*** interface.
`ip http server`	Enables HTTP server on the ISR G2, allowing clients to communicate with the router using HTTP when passing authentication credentials. **Note:** Credentials can be passed using HTTPS instead of HTTP with the ip http secure-server command. With this, clients may encounter SSL certificate errors, as the ISR uses a test certificate server. To avoid SSL certificate errors, replace the certificate on the ISR with a certificate signed by a trusted certificate authority.

Transparent Authentication with NTLM

When the ISR uses NTLM to authenticate users, it tries to retrieve user credentials transparently from the client application without prompting end users for information. If the client application cannot send user credentials transparently, it prompts users to enter their username and password.

When the ISR performs NTLM authentication, it redirects the client browser from the originally requested URL to the virtual proxy URL configured on the ISR (by either address or host name, whichever is configured). Once the browser redirects users to the virtual proxy URL, they are prompted for authentication credentials. When they are successfully authenticated, they are redirected back to the originally requested URL.

Users can be transparently authenticated using NTLM when they access the web from some web browsers on a Windows operating system. For example, they can be transparently authenticated from Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome on Windows, but they will be prompted for authentication credentials on MacOS and on Apple Safari and Opera on any operating system.

However, to ensure that users are transparently authenticated using Internet Explorer, Firefox, and Chrome on Windows, you must complete the following steps:

1. Define a virtual proxy URL on the ISR, using the ip admission command, by either IP address (virtual-ip subcommand) or host name (virtual-host subcommand).

   For example, to define both an IP address and a host name for the virtual proxy URL, use the following command:

   ```
   ip admission virtual-ip 1.1.1.1 virtual-host webproxy
   ```

Note: You can specify any single-word host name as the virtual proxy host name. The virtual proxy IP address must not be used by any existing device and cannot be an IP address that is already used on the ISR G2 router.

2. Configure the third-party software to ensure that it transparently authenticates users using the virtual proxy URL.

- **Internet Explorer and Chrome:** Perform either of the following steps:

If a virtual proxy host name is defined, you can create a DNS A record resolving the virtual proxy host name specified in step 1 (webproxy) to the virtual proxy IP address specified in step 1 (1.1.1.1).

This method works because Internet Explorer and Chrome consider a single-word host name to be a local intranet server.

Or:

Add the virtual proxy URL to the Internet Explorer Local Intranet Zone.

If only the virtual proxy IP address is defined, add its IP address (for example, http://1.1.1.1) to the Local Intranet Zone.

If the virtual proxy host name is defined, add its host name (for example, http://webproxy) to the Local Intranet Zone.

For more information on adding a URL to the Internet Explorer Local Intranet Zone, see the Internet Explorer documentation.

- **Firefox:** Edit the Mozilla Firefox preference that determines which sites are allowed to automatically authenticate using NTLM, and add the virtual proxy URL configured in step 1.

  Typically, this is the “network.automatic-ntlm-auth.trusted-uris” configuration setting. For more information on editing the Firefox configuration, see your Firefox documentation, or search online.

Bypassing Authentication

In some circumstances, you may want only a certain subset of users to be asked for authentication. In this case, you can use network/IP-based or browser-based authentication bypass to disable the authentication prompt to end users.

Network/IP-Based Authentication Bypass

To configure the ISR G2 to bypass authentication for certain subnets and users, you must know the IP addresses either of the users you do want to authenticate or of the users you do not want to authenticate.

The basic idea is to create an ACL “permitting” users you want to ask for authentication and “denying” users you want to bypass authentication. Then tie this ACL to the ip admission command.

For example, if you know the IP addresses of the users you want to authenticate:

```
ip access-list extended authenticationACL
 !! users in this IP range will be asked to authenticate first
 permit ip 10.0.0.0 0.0.0.255 any any
 !! everyone else bypasses authentication
 !! [implicit deny for all others]

ip admission name ntlm-rule ntlm list authenticationACL
```

If you know the IP addresses of users you **don’t** want to authenticate:

```
ip access-list extended authenticationACL
 !! users in this IP range will be NOT be asked to authenticate
```

```
 deny ip 10.0.0.0 0.0.0.255 any any
 !! everyone else must authenticate first
 permit ip any any

ip admission name ntlm-rule ntlm list authenticationACL
```

Note: The above configuration is typically used only in proof-of-concept or pilot phases, where only a subset of all users will be using Cisco Cloud Web Security. For production deployments, typically all corporate users would be asked to authenticate. For guest users, it is recommended to have a separate VLAN or network for guest access where authentication is not applied. The bypass authentication configuration described above should be used only if a separate guest VLAN/network is not possible.

Browser-Based Authentication Bypass

Transparent authentication with no pop-up prompts to enter user credentials can be achieved with NTLM authentication. However, there may still be pop-up prompts for some browsers that do not handle transparent NTLM authentication, such as Firefox or Safari. To prevent pop-ups from appearing in these browsers, you can bypass user authentication based on the browser used.

This bypass feature uses the user agent string sent by the browser. A list of user agent strings can be configured on the browser. Before authentication, the ISR G2 checks whether the user agent string from the end user's device matches one of the configured user agent strings. If there is a match, authentication is bypassed, and the user is able to access the Internet with guest Cloud Web Security policies. If there is no match, user authentication is required. With browsers that support transparent NTLM authentication, this authentication will happen in the background, and the user will not see a prompt for credentials.

Note: The ISR G2 does a string match on the user agent string configured on the router with the user agent string sent by the browser. A browser can change the user agent string that it uses to identify itself at any time. Cisco has no control over this. Administrators must keep the list of user agent strings on the ISR G2 up to date. To find the user agent string your browser is sending, see http://whatsmyuseragent.com/. A list of user agent strings can also be found online at sites such as http://techpatterns.com/forums/about304.html.

Use the commands in Table 6 to configure browser-based authentication bypass.

Table 6. Configuring Browser-Based Authentication Bypass

Command	Description
`parameter-map type regex <parameter-map name>`	Configures regular expressions parameter map.
`pattern <pattern string>`	Configures a matching pattern in the user agent field of the browser.
`ip admission name <rule name> bypass regex <parameter-map name>`	Adds the bypass rule to the ip admission command.
`ip admission name <rule name> bypass absolute-timer <0-35791>`	Sets the timer for browser-based authentication bypass sessions.

The following is a sample user agent string for an iPad 3:

“Mozilla/5.0 (iPad; CPU OS 5_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B176 Safari/7534.48.3”

Most smartphones or tablets will have the following user agent strings:

Mobile = iphone|ipod|android|blackberry|opera|mini|windows\sce|palm|smartphone|iemobile

Tablet = ipad|android|android|xoom|sch-i800|playbook|tablet|kindle

The following is a sample parameter map (to match common user-owned devices) that uses the user agent strings given above:

```
parameter-map type regex byod
 pattern .*iPad*
 pattern .*andriod*
 pattern .*kindle*
```

Authentication Failure

Prior to the 15.2(4)M3 release, if the user failed authentication, the default behavior was to block all Internet access for that IP address. This was not configurable, although you could configure the timeout value so that the user could try again after the timer expires. In Release 15.2(4)M3 and later, however, if the user fails authentication, configurable guest access policies apply.

Note: The following are causes of user authentication failure:

- The user entered a wrong username and password (the user cannot click the Cancel button in the NTLM pop-up window or hit Enter without entering any characters) AND one of the following conditions apply:
  - The username, password, or both are incorrect in active NTLM authentication mode
  - The username is incorrect in passive NTLM authentication mode
- The LDAP server is not reachable.

In this case, the user needs to try at least five times, or the configured number of maximum login attempts, before the failure occurs.

For images that support the feature, there are no additional configurations to enable default guest access; it is enabled by default. However, it is important to configure the maximum number of login attempts required before a user falls back to the default guest access policy. By default, the maximum login attempt value is 5. This means that a user must fail five consecutive login attempts before falling back to the default access policy.

To change the max-login-attempt value, configure the command shown in Table 7.

Table 7. Configuring the Maximum Number of Login Attempts

Command	Description
`ip admission max-login-attempt <1-2147483647>`	Configures the maximum number of login attempts required before falling back to the default guest policy.

For example, for a user to automatically connect to the network with guest policies after two failed login attempts, use the following command:

```
ip admission max-login-attempt 2
```

When determining the maximum login attempt value, understand the risks of corporate users entering the wrong username and password. If the value is too low, some corporate users may be moved to the default guest policy with multiple authentication pop-up messages. We recommend that you configure a maximum login attempt value of at least 2 to prevent corporate users from being authenticated as guests very often.

Session States and Time Between Sessions

If a user fails authentication, that user is authenticated as a guest user by using the configured default guest policy; however, the session state will show SERVICE_DENIED. The session will remain in SERVICE_DENIED state for a default of two minutes, after which the session is moved to the initialized (INIT) state and the user will be prompted for credentials.

To adjust the time between authentication prompts, enable a watch list and configure the watch-list timeout:

```
ip admission watch-list enable
ip admission watch-list expiry-time [time in minutes]
```

For example, to ensure that a user does not get prompted for credentials again within 24 hours, configure the following command:

```
ip admission watch-list enable
ip admission watch-list expiry-time 1440
```

Note: We recommend not setting the watch-list expiry timer to a very high value, as doing so will prevent prompting for credentials until the timer expires.

Domain and Nondomain Users

Domain users who use transparent NTLM authentication with supported browsers cannot log in to the domain with invalid credentials. Because the device/domain will not let a user log in to a network with invalid credentials, the domain will always have the correct username and user group, which ensures that the user always receives the granular user policies defined in the Cloud Web Security portal. If a user's password expires, the user must log off and log back in to the domain with the new password.

The default guest access policy is available to users who use nontransparent NTLM authentication methods and fail authentication.

Note: The following types of users are considered to be nondomain users:

- Domain users who do not use either Internet Explorer or Chrome (which supports transparent NTLM by default)
- Any user logging in to a device locally (such as workgroup machines supporting local sign-on)
- Guest users

During authentication, nondomain users must specify the domain name (cisco\jdoe) and the password. If a user enters only the username and password, the client PC considers the host name/computer name as the domain name and the user may not be authenticated, even when proper credentials were given.

For example, a Cisco corporate user John Doe using a Mozilla Firefox browser (which does not support transparent NTLM authentication by default) works under the “ciscoeurope” domain. The user will need to log in with username “ciscoeurope\jdoe” to be recognized as a corporate user with the proper corporate policies from Cloud Web Security. If the user enters only “jdoe” to log in to a machine under the “cisco” domain, the username passed will be “cisco\jdoe.” This would result in the user eventually being authenticated as a guest user with the default policy applied.

Acceptable Use Policy Agreement

You can also configure the ISR so that users accessing the web must agree to an acceptable use policy before browsing the web. This authentication helps warn users that their web traffic is scanned by Cisco Cloud Web Security.

Acceptable use policy (AUP) agreement enforcement works with and without authentication. However, the only authentication type supported with AUP on the ISR G2 is Web authentication. NTLM and HTTP Basic authentication are not supported.

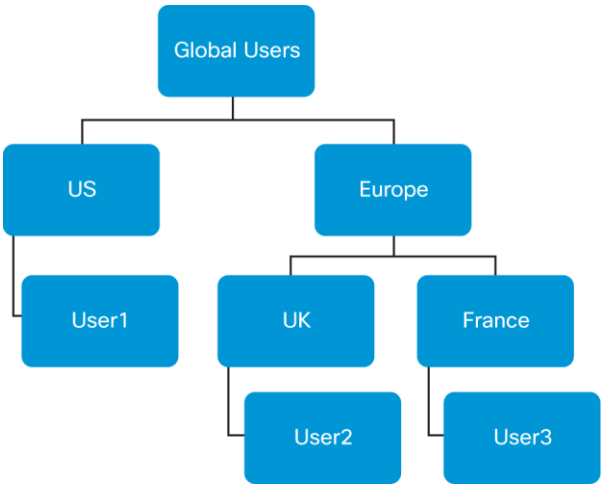
To require users to agree to the acceptable use policy agreement, use the Consent feature. For more information, go to the Consent Feature for Cisco IOS Routers page.

Nested LDAP

In Cisco IOS Release 15.3(3)M and later, nested LDAP is supported with HTTP Basic, Web, and NTLM authentication. With this support, the LDAP client module will fetch both direct and nested user-group information for a use.

Figure 1 provides an overview of how nested LDAP works with Cloud Web Security.

Figure 1. Nested User-Group Information



Consider the simple representation of an Active Directory tree in Figure 1.

If nested LDAP is not enabled, users 1, 2, and 3 would show up as members of the following groups:

- User1 is a member of Group (US).
- User2 is a member of Group (UK).
- User3 is a member of Group (France).

If nested LDAP is enabled, users 1, 2, and 3 would show as members of the following groups:

- User1 is a member of Group (GlobalUsers, US).
- User2 is a member of Group (GlobalUsers, Europe, UK).
- User3 is a member of Group (GlobalUsers, Europe, France).

Nested-level search occurs within the base domain scope specified in the LDAP server configuration. For instance, if the base domain is specified as “Europe,” User2 and User3 would not show up as members of the GlobalUsers group.

Use the command shown in Table 8 to enable or disable nested LDAP search.

Table 8. Configuring Nested LDAP Search

Command	Description
`ldap server <server name>` `[no] search-type nested`	Configures the maximum number of login attempts required before falling back to the default guest policy.

When nested LDAP is enabled, it is important to note that performance is directly related to the level of nested depths and users in the Active Directory domain. Nested LDAP lookup requires a recursive search through the Active Directory domain until the last node is found and therefore may introduce latency in the authentication process compared to non-nested LDAP search.

For optimal performance, a nested Active Directory depth of no more than four or five levels is recommended. In addition, it is recommended that you increase the server timeout value, because there may be an increase in the time it takes for all groups to be fetched. A timeout retransmit value of 60 (from the default of 30 seconds) is recommended for nested LDAP searches.

Use the subcommand shown in Table 9 to change the LDAP server timeout value.

Table 9. Configuring the LDAP Server Timeout Value

Command	Description
`ldap server <server name>` **`timeout retransmit 60`**	Changes timeout retransmit value to 60 seconds; recommended for nested LDAP searches. (Default is 30 seconds.)

Configuring the Cisco Cloud Web Security Portal

Configure Cloud Web Security using its web-based GUI portal.

To configure Cisco Cloud Web Security to work with the ISR, you must complete the following steps:

1. Create a Cloud Web Security authentication key.

   For more information, see the next section, Creating a Cisco Cloud Web Security Authentication Key.

2. Define Cloud Web Security user groups.

   For more information, see the Defining Cisco Cloud Web Security User Groups section in this document

3. Create Cloud Web Security web policies.

   For more information, see the Creating Cisco Cloud Web Security Policies section in this document.

4. Configure the Malware Service options in the Cloud Web Security portal.

   For more information, see the Malware Service chapter in the *Cloud Web Security Portal Administrator Guide* at http://www.cisco.com/en/US/docs/security/web_security/scancenter/sc5200a/Malware.html.

5. View reports in the Cloud Web Security portal.

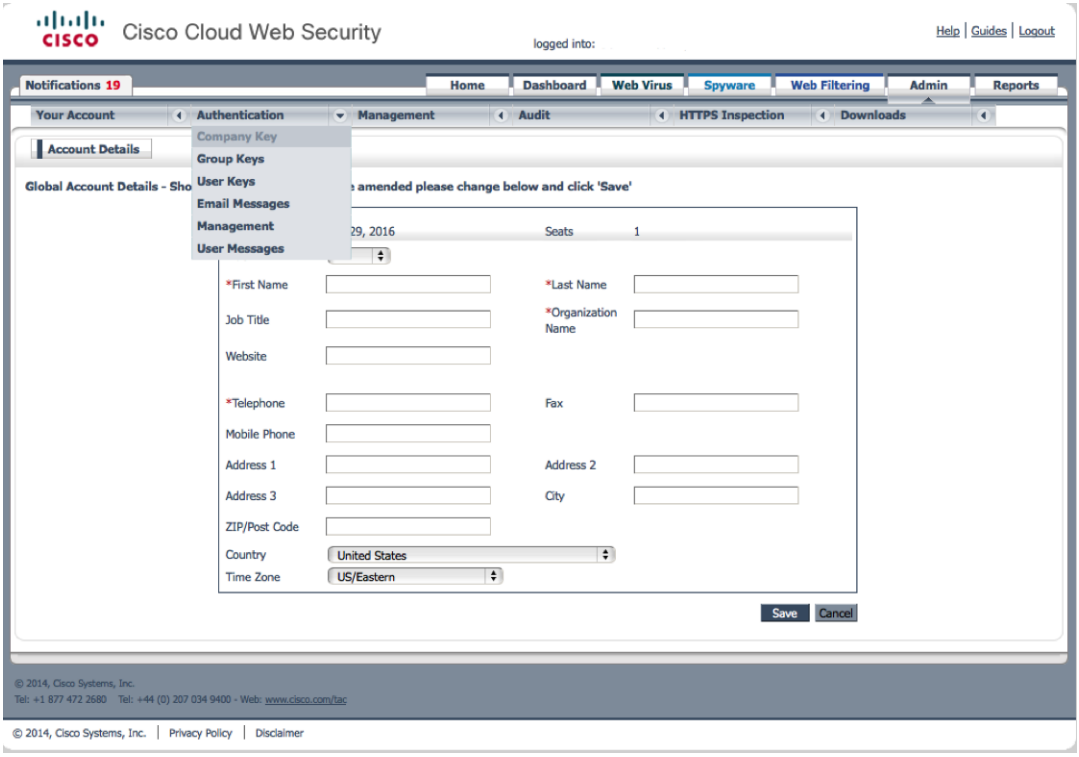
   For more information, see the Reporting chapter in the *Cloud Web Security Portal Administrator Guide* at http://www.cisco.com/en/US/docs/security/web_security/scancenter/sc5200a/Reporting.html.

Creating a Cisco Cloud Web Security Authentication Key

In the Cloud Web Security portal, navigate to the Admin page and create either a company or group authentication key. The type of key you create depends upon your network environment. For more information on the type of key to create, see the Working with Multiple ISRs section in this document.

Figure 2 shows where you can create and edit a company key on the Admin page.

Figure 2. Creating a Company Key in the Cloud Web Security Portal



For more information on how to create keys in the Cloud Web Security portal, see the “Authentication” section of the Administration chapter in the Cloud Web Security Portal Administrator Guide at http://www.cisco.com/en/US/docs/security/web_security/scancenter/sc5200a/Administration.html - wp1071241.

Defining Cisco Cloud Web Security User Groups

If the ISR enforces authentication and you want to create different web policies for each user group, or if you have configured a different group key for different ISRs, you need to define user groups in the Cloud Web Security portal.

You can define the following types of groups:

- **Directory:** Directory groups can be Windows Active Directory groups or LDAP groups.
- **Custom:** Custom groups enable you to create a group containing any users, regardless of their active directory or LDAP group.

In the Cloud Web Security portal, create user groups on the Admin page. For more information, see the “User Management” section of the Administration chapter in the *Cisco Cloud Web Security Portal Administrator Guide* at http://www.cisco.com/en/US/docs/security/web_security/scancenter/sc5200a/Administration.html - wp1056123.

Creating Cisco Cloud Web Security Policies

ScanCenter’s Web Filtering Service enables you to create different web policies to enforce acceptable use policies for web traffic. To create a policy, you must first configure web filters and schedules that apply to policies. Web filters are used to control content passing into the network. Schedules are used to determine when policy rules are applied.

Configure web filters, schedules, and policies on the Web Filtering page in ScanCenter. For more information on configuring these objects, see the Web Filtering Categories document.

Helpful CLI Commands

Show Commands

Cisco IOS includes other CLI commands you can use to manage and troubleshoot the content-scanning process on the ISR (Table 10).

Table 10. Commands Related to the Content-Scanning Process on the ISR

Command	Description
`show content-scan session active`	Displays all active content-scanning process sessions.
`show content-scan session history <1-512>`	Displays the history of content-scanning process sessions; up to 512 terminated sessions.
`show content-scan statistics`	Displays content-scanning process statistics.
`show content-scan summary`	Displays generic details related to Cloud Web Security, such as active/standby information, etc. The * signifies the chosen active server.
`debug content-scan {function-trace | event | packet | error}`	Enables the debug messages, which display content-scanning process function traces, events, packet flow, and errors.
`clear content-scan statistics`	Clears content-scanning process statistics.

Logging Messages

Enabling Cisco Cloud Web Security Logging

Cisco Cloud Web Security logging is enabled via a subcommand under the content-scan parameter map (Table 11).

Table 11. Configuring Cloud Web Security Logging

Command	Description
`parameter-map type content-scan global`	Configures parameters for Cloud Web Security on the ISR G2.
`logging`	Subcommand enabling Cloud Web Security logging.

The syslogs in Cisco IOS include messages that relate to the content-scanning process. Table 12 lists the syslog messages.

Table 12. Syslog Messages Related to the Content-Scanning Process

Command	Description
`%CONT_SCAN-6-START_SESSION`	Indicates that a flow is created by the content-scanning process. This syslog message is rate-limited.
`%CONT_SCAN-6-STOP_SESSION`	Indicates that a flow is removed by the content-scanning process. This syslog message is rate-limited.
`%CONT_SCAN-3-CONNECTIVITY`	Indicates that the primary or secondary Cloud Web Security proxy server is up or down. When the server is up, the “is up” message appears only after the configured timeout value, which by default is 300 seconds.

Command	Description
%CONT_SCAN-3-UNREACHABLE	Indicates that both the primary and secondary Cloud Web Security proxy servers are down and that the content-scanning process is disabled.
%CONT_SCAN-3-TOWER-CHANGE	Indicates that a new Cloud Web Security proxy server is selected as the primary server.
%CONT_SCAN-6-WHITE_LIST	Indicates that a flow is scanned by Cloud Web Security because the original client request matched the configured whitelist. The message includes the reason for the client request matching the whitelist. This syslog message is rate-limited.

Sample Configuration

The following is a sample Cloud Web Security configuration with NTLM authentication:

```
! Cloud Web Security parameter-map features
parameter-map type content-scan global
 server scansafe primary ipv4 72.37.244.115 port http 8080 https 8080
 server scansafe secondary ipv4 80.254.152.99 port http 8080 https 8080
 license 0 5D22AA983ABC544AF92F83A51A507262 ! Copied from ScanCenter
 source interface GigabitEthernet0/0
 timeout server 30
 user-group cisco username ciscouser
 server scansafe on-failure block-all

! Enable Cloud Web Security on outbound interface
interface GigabitEthernet0/0
 description outbound interface
 content-scan out

! Cloud Web Security whitelist parameters
content-scan whitelisting
 whitelist acl name whitelistedSubnets
 whitelist header host regex whitelist

! Whitelist pattern parameter-map
parameter-map type regex whitelist
 pattern google
 pattern cisco
```

```
! Whitelist ACL
ip access-list standard whitelistedSubnets
 permit 10.1.0.0 0.0.0.255

! Define LDAP attribute map
ldap attribute-map ad-map
 map type sAMAccountName username

! Configure LDAP server
ldap server ss
 ipv4 10.0.0.1
 attribute map ad-map
 bind authenticate root-dn CN=CiscoScansafe,OU=Global, DC=Cisco,DC=com password 0
secretpassword ! optional
 base-dn DC=Cisco,DC=com

! Enable authentication commands
aaa new-model

! Define AAA group and add LDAP server to the group
aaa group server ldap ss-grp
 server ss

! Define AAA authentication and authentication groups
aaa authentication login aaa-ss group ss-grp
aaa authorization network aaa-ss group ss-grp

! Define IP admission rules, in this case, with NTLM authentication and specific
subnet of IPs subject to authentication only
ip admission name ntlm-rule ntlm absolute-timer 60 list authlist
ip admission name ntlm-rule method-list authentication aaa-ss authorization aaa-
ss

! Enable authentication on inbound interface
interface GigabitEthernet0/1
 description inbound interface
 ip admission ntlm-rule

! Define max login attempts. User must fail login 2x before falling back to
default guest policy
ip auth-proxy max-login-attempts 2

! Enable IP admission watch list
ip admission watch-list enable
```

```
! Define watch-list timer. Users on watch list will not be reprompted for
authentication for 24 hours
ip admission watch-list expiry-time 1440

! Define virtual IP and virtual host name for NTLM transparent authentication
ip admission virtual-ip 1.1.1.1 virtual-host CWSwebproxy

!! Configure Cloud Web Security authentication bypass. ACL will bypass defined
subnets for authentication only. Cloud Web Security is still applied for these
networks.
ip access-list extended authlist
 permit ip 10.0.1.0 0.0.0.255 any any ! these subnets have to do authentication
 [implicit deny for all others] ! all other IPs bypassed
```

Tech Tips

Packet drops with small Maximum Transmit Unit (MTU) value on interfaces

Although very rare, there is a chance that small MTU values (ip mtu <mtu value> under the interface subcommand) configured on any interface in the network may prevent web browsing. Packets may be dropped, preventing browsing, if the packet size is greater than the MTU size specified on the interface and the packet is being sent with a “do not fragment” (DF) bit set.

The workaround for this is to configure ip tcp adjust-mss <segment size> on the interface along with the ip mtu <mtu value> command. The value for the segment size should be less than the MTU value minus 40.

For example:

```
interface FastEthernet4
 ip mtu 100
 ip tcp adjust-mss 55
```

Different local web pages when Cloud Web Security tower is located in a different country than the user

While Cisco Cloud Web Security will always choose the best tower for your geographical location, at times there may not be a tower that exists in the same country where users are located. In this case, web pages that use localization features or have a local server may not display the proper local features if the Cloud Web Security tower is not located in the same country as the user.

For example, if your users are located in the United States, but your tower is located in the United Kingdom (U.K.), entering www.yahoo.com may redirect the user to www.yahoo.co.uk since the returning traffic from the Cloud Web Security tower originates from the U.K.

The workaround for this is to enter the specific country URL. For example, in the above situation, entering www.us.yahoo.com would take the user to the proper local Yahoo! site.

Host- and user agent-based whitelisting inconsistencies with asymmetric routing

The host- and user agent-based whitelisting may not work properly with asymmetrical routing since the returning SYN-ACKs takes a different path than the initiating SYN.

The workaround for this is to use IP-based whitelisting instead of header-based whitelisting.

Page loads differently after Cloud Web Security warning page

When the Warning option is used, the destination page may load differently than normal after the user clicks "Accept." This is a known issue. Functionality of the page should not be lost; it is only appearance that is affected.

Virtual host name resolves to open DNS server

If the virtual host name is configured incorrectly, it is possible that the virtual host name will resolve to the open DNS server. While this does not affect functionality in any way, it could be seen as a security risk in some circumstances. To avoid this, check the virtual IP address with the virtual host name to ensure that it is configured correctly.

NTLM authentication and browser-based authentication bypass supports only GET requests

The NTLM authentication and browser-based authentication bypass feature on the ISR G2 currently supports only the GET method in the HTTP request. Other methods such as POST, PUT, etc. are not supported, and the ISR G2 will close connections if one of these unsupported methods is received prior to authentication.

This means that should the authentication timer expire while a user is completing a form, for example, the form may not be submitted correctly. (Since submission uses a POST method, the HTTP request would include the POST request, and the ISR would subsequently close that connection.) To avoid this, simply open another page or link using a GET method.

Clearing the IP admission cache may result in additional NTLM pop-ups

If an administrator issues the clear ip admission cache command on the ISR G2, it will clear all the established sessions for a particular user (or for everyone, depending on what the administrator configures). As a result, if NTLM authentication is configured, some users may see additional pop-ups requesting credentials. This would be most noticeable if authentication timers are configured for longer periods of time and users are typically not expecting to get credential prompts frequently.

To reduce the chance of more people getting pop-ups, issue the clear ip admission cache command during non-peak hours, if possible. Also, if only certain users need their sessions cleared, indicate their specific IP address using clear ip admission cache <ip addr> to avoid clearing everyone else's sessions.

Multiple NTLM authentication pop-ups when virtual IP not configured

NTLM authentication may not appear transparent to the end user if the virtual IP is not configured.[1] To avoid this, configure the virtual IP and virtual host name, and make sure they are resolvable in the DNS.

Root bind in LDAP configuration required for NTLM passive authentication

The root bind CLI under the LDAP server configuration (bind authenticate root-dn <attributes>) is mandatory in order for NTLM passive authentication to work. With NTLM active authentication, the root bind is optional.

Protecting the ISR G2 from Layer 4 Forwarding level attacks

The Cloud Web Security connector on the ISR G2 may be prone to Layer 4 level TCP attacks. To protect the ISR Cloud Web Security solution from various Layer 4 level attacks, use features such as zone-based firewall or IPS to detect and prevent some attacks.

[1] Not all browsers and operating systems will support transparent NTLM authentication. See the Cisco Cloud Web Security Design Guide for a table of supported browsers and operating systems for transparent NTLM authentication.

Cloud Web Security whitelisting does not support ACL logging

The ACL for Cloud Web Security IP-based whitelisting does not support ACL logging (that is, an ACL statement such as “permit ip host 1.1.1.1 any log” is not supported). Use ACLs without the log keyword enabled.

Cloud Web Security and Multipath TCP

Cloud Web Security does not currently support Multipath TCP (MTCP). For devices using MTCP, such as Apple devices running iOS 7, the MTCP feature will be disabled.

Additional Documentation

This document is intended to serve as an overview of the entire Cisco ISR with Cisco Cloud Web Security solution. It does not include detailed steps for configuring each product component, nor does it list all potential interactions with other features of each component. For detailed information on how to install, configure, and upgrade each component in the solution, see the release notes and user guides for each product.

Cisco Cloud Web Security documentation home page:
http://www.cisco.com/c/en/us/support/security/cloud-web-security/tsd-products-support-series-home.html

Cisco ScanCenter Administrator Guide:
Cisco ScanCenter Administrator Guide

Cisco IOS 15.2M&T documentation home page:
http://www.cisco.com/en/US/products/ps11746/tsd_products_support_series_home.html

Security Configuration Guide: Cisco Cloud Web Security Cisco IOS Release 15M&T:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_cws/configuration/15-mt/sec-data-cws-15-mt-book.html

A complete list of the Securing the Data Plane configuration guides, including the Zone-Based Policy Firewall document:
http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/security/config_library/15-mt/secdata-15-mt-library.html

A complete list of the Cisco IOS Security Command Reference documents listed under the “Security and VPN” section:
http://www.cisco.com/en/US/products/ps11746/prod_command_reference_list.html

Support

For issues related to the Cisco ISR G2 or Cisco Cloud Web Security, open a case with Cisco TAC:
http://tools.cisco.com/ServiceRequestTool/create/launch.do

This document is to be used in conjunction with the documents listed in the “Additional Documentation” section.

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 C07-732662-00 09/14