Configuring NTLM Authentication on the Cisco 4000 Series ISRs

This document describes how to configure NTLM Authentication on Cisco 4000 Series ISRs. The Cisco 4000 Series ISRs with NTLM Authentication and Cloud Web Security solution can enable branch offices to intelligently redirect web traffic to the cloud to enforce granular security 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.

Contents

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Cisco Systems, Inc.
www.cisco.com

Restrictions and Limitations

This section describes limitations and restrictions for this feature.

- IPv6 is not supported
- Interoperability with VRFs is not supported

Information about NTLM Basic Authentication

Cisco 4000 Series ISR uses Windows NT Lan Manager (NTLM) to retrieve user credentials transparently from the client application without prompting end users for authentication. If the client application cannot send user credentials transparently, Cisco 4000 Series ISR prompts users to enter credentials. When using NTLM authentication, you can choose two modes: active or passive. The default mode for NTLM authentication is active. To enable passive mode, configure the command ip admission name rule1 ntlm passive.

In NTLM active mode, Cisco 4000 Series routers gather both the username and password from the client during the TCP handshake process and verify these against the Active Directory domain controller. In NTLM passive mode, Cisco 4000 Series routers only query for the user group information and do not verify the password, which reduces the number of transactions between Cisco 4000 Series routers and the domain controller.

Configuring the NTLM Authentication

To configure the NTLM authentication, perform these steps.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **ldap server** *ldap-server-name*
5. **ipv4** *ip-address*
6. **base-dn** *string*
7. **search-filter user-object-type top**
8. **authentication bind-first**
9. **exit**
10. **aaa group server ldap** *group-name*
11. **server** *ldap-server-name*
12. **aaa authentication login default group** *group-name*
13. **aaa authorization network default group** *group-name*
14. **ip admission name** *admission-name* **ntlm | passive | list** *access-list* **| absolute-timer** *absolute-time in minutes* **| inactivity-time** *inactivity-time in minutes*|
15. **ip admission virtual-ip** *ip-address* **virtual-host** *hostname*

16. **interface type** *number*
17. **ip admission** *admission-name*
18. **exit**
19. **ip http server**
20. **ip http secure-server**
21. **ip admission absolute-timer** *absolute-time in minutes*
22. **ip admission inactivity-timer** *inactivity-time in minutes*
23. **ip admission init-state-time** *init-state-time in minutes*
24. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**aaa new-model** Example: `Router(config)# aaa new-model`	Enables the authentication, authorization, and accounting (AAA) functionality on the device. **Note** Once you enable the aaa new-model command, it cannot be disabled.
Step 4	**ldap server** *ldap-server-name* **Example:** `Router(config-if)#ldap server server1`	Defines a Lightweight Directory Access Protocol (LDAP) server and enters LDAP server configuration mode.
Step 5	**ipv4** *ip-address* **Example:** `Router(config -ldap-server)# ipv4 10.1.1.1`	Specifies the LDAP server IP address using IPv4.

	Command or Action	Purpose
Step 6	**base-dn** *string* **Example:** `Router(config-if -ldap-server)# base-dn "dc=sns,dc=example,dc=com"`	(Optional) Configures the base distinguished name to use for search operations in the LDAP server..
Step 7	**search-filter user-object-type top** **Example:** `Router(config-if -ldap-server)# search-filter user-object-type top`	Specifies the search filter to be used in the search requests.
Step 8	**authentication bind-first** **Example:** `Router(config -ldap-server)# authentication bind-first`	Configures the sequence of search and bind operations for an authentication request.
Step 9	**exit** **Example:** `Router(config -ldap-server)# exit`	Exits mode and returns to global configuration mode..
Step 10	**aaa group server ldap** *group-name* **Example:** `Router(config)# aaa group server ldap name1`	Defines the AAA server group with a group name and enters LDAP server group configuration mode. All members of a group must be the of same type, that is, RADIUS, LDAP, or TACACS+.
Step 11	**server** *ldap-server-name* **Example:** `Router(config-if)# server server1`	Defines the AAA server group and enters LDAP server group configuration mode.

	Command or Action	Purpose
Step 12	**aaa authentication login default group** *group-name* **Example:** `Router(config)# aaa authentication login default group name1`	Sets AAA authentication at login. The default keyword uses the listed authentication methods that follow this keyword as the default list of methods when a user logs in.
Step 13	**aaa authorization network default group** group-name **Example:** `Router(config)# aaa authorization network default group name1`	Defines the AAA authorization with a network default group name.
Step 14	**ip admission name** *admission-name* **ntlm** | **passive** | **list** *access-list* | **absolute-timer** *absolute-time in minutes* | **inactivity-time** *inactivity-time in minutes*| **Example:** `Router(config)# ip admission name [test] ntlm | passive | list 100 | absolute-timer 60 | inactivity-time 20`	Configures NTLM (Active/Passive) authentication rule with the options to specify the subnet to be subjected to authentication and the time for which authenticated sessions can remain active or can remain active without any activity.

Step 15	**ip admission virtual-ip** *ip-address* **virtual-host** *hostname*
	
	Example:
	`Router(config)#`
	`ip admission virtual-ip 10.2.2.2 virtual-host webproxy`
		Configures a NTLM Authentication virtual-ip and virtual-host.
		• The Virtual-host is required only for transparent NTLM authentication.
		• The Virtual-IP address should not correspond to an existing device on the network and should not be configured on any interface on the Cisco 4000 Series ISR. The virtual-host is a single-word, non-qualified domain-name.

Step 16	**interface type** *number* **Example:** `Router(config)# interface gigabitethernet 0/0`	Configures an interface and enters interface configuration mode.

	Command or Action	Purpose
Step 17	**ip admission** *admission-name* **Example:** `Router(config)# ip admission test`	Applies the NTLM Authentication rule on the interface.
Step 18	**exit** **Example:** `Router(config)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 19	**ip http server** **Example:** `Router(config)# ip http server`	Credentials can be passed using HTTPS instead of HTTP with the command ip http server. With HTTPS, clients may encounter SSL certificate errors as the Cisco 4000 Series routers use a test certificate server. To avoid SSL certificate errors, replace the certificate on Cisco 4000 Series routers with a certificate signed by a trusted certificate authority.
Step 20	**ip http secure-server** **Example:** `Router(config)# ip http secure-server`	Credentials can be passed using HTTPS instead of HTTP with the command ip http secure-server. With HTTPS, clients may encounter SSL certificate errors as the Cisco 4000 Series routers use a test certificate server. To avoid SSL certificate errors, replace the certificate on Cisco 4000 Series routers with a certificate signed by a trusted certificate authority.
Step 21	**ip admission absolute-timer** *absolute-time in minutes* **Example:** `Router(config)# ip admission absolute-timer 305`	Configures specified absolute timeout globally that is applicable for all the NTLM authentication rules.
Step 22	**ip admission inactivity-timer** *inactivity-time in minutes* **Example:** `Router(config)# ip admission inactivity-timer 205`	Configures specified inactivity time globally that is applicable for all the NTLM authentication rules.

	Command or Action	Purpose
Step 23	**ip admission init-state-time** *init-state-time in minutes* **Example:** `Router(config)# ip admission init-state-timer 15`	Configures specified init-state time globally that is applicable for all the NTLM authentication rules.
Step 24	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Transparent Authentication with NTLM

Users are transparently authenticated by using NTLM when they access the web using a web browsers on the Windows operating system. For example, users are transparently authenticated through Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome on Windows; however, the users are prompted for authentication credentials when using Apple Safari on an Apple Macintosh or Opera on any operating system.

To ensure that users are transparently authenticated using Microsoft Internet Explorer, Mozilla Firefox, and Chrome on the Windows operating system, perform the following steps:

1. Define a virtual-ip and a virtual-host (resolvable to virtual-ip) on the Cisco 4000 Series ISR using the **ip admission** command.

```
ip admission virtual-ip 10.1.1.1 virtual-host webproxy
```

Note You can specify a single-word hostname as the virtual-host. The virtual-ip must not be used by any other device or configured on the Cisco 4000 Series ISR.

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

- For Internet Explorer and Chrome, perform either of the following steps:
  - If a virtual-host is defined, you can create a DNS A record resolving the virtual-host specified in Step 1 (webproxy) to the virtual-ip specified in Step1 (10.1.1.1).This method works because Internet Explorer and Chrome consider a single word hostname as a local intranet server. Or
  - Add the the virtual-ip/virtual-host to the Internet Explorer Local Intranet Zone. If only the virtual-ip is defined, then add its IP address (for example, http://10.1.1.1) to the Local Intranet Zone. If the virtual-host is defined, then add its hostname (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.

- For Firefox, edit the Mozilla Firefox preference that determines which sites are allowed to automatically authenticate using NTLM and add the virtual-ip/virtual-host 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

Use network/IP-based or browser-based authentication bypass to disable the authentication for users.

Network/IP-Based Authentication Bypass

To configure Cisco 4000 Series ISR router to bypass authentication for certain subnets and users, you must either know the IP addresses of the users you do want to authenticate, or the IP addresses of users you do not want to authenticate. Create an ACL to permit user authentication or deny user authentication. The ACL rule must associated with the ip admission command.

The following example shows how to authenticate users whose IP addresses are known:

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

The following example shows how not to authenticate users whose IP addresses are known:

```
ip access-list extended authenticationACL
 deny ip 10.0.0.0 0.0.0.255 any any  !! users in this IP range will be NOT be asked to
authenticate. everyone else must authenticate first
 permit ip any any
!

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

Note This configuration is mostly used only in proof-of-concept or pilot phases where only a subset of users access Cisco Cloud Web Security. For production deployments, typically all corporate users are asked for authentication. For guest users, it is recommended to have a separate VLAN or a network that does not apply authentication. The bypass authentication configuration should only be used if a separate guest VLAN/network is not possible.

Browser-Based Authentication Bypass

Transparent authentication can be done through NTLM authentication. However, some web browsers that do not support transparent NTLM authentication, such as Mozilla Firefox or Apple Safari, will use authentication prompts.

The Browser-Based Authentication Bypass features uses the user agent string sent by the web browser to bypass authentication. A list of user agent strings can be configured on the Cisco 4000 Series ISRs. Before the authentication, the Cisco 4000 Series ISRs checks if the user agent string from a user's device matches the configured list. If there is a match, authentication is bypassed, and the user can access the Internet with guest Cloud Web Security policies. If there is no match, user authentication is required. Web browsers that support transparent NTLM authentication, the authentication happens in the background, and users are not prompted for credentials.

The Cisco 4000 Series ISR does a match on the user agent string configured with the user agent string sent by the web browser. Web browsers may change the user agent string that is used to identify the browser. As a best practice, the Network administrators should periodically update the list of user agent strings on the Cisco 4000 Series ISR router. To find the user agent string that your web browser is sending, go to http://whatsmyuseragent.com. A list of user agent strings is also available at http://techpatterns.com/forums/about304.html

A sample user agent string for an iPad 3 would be the following: "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"Typically most smartphones or tablets 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
```

Use the commands below to configure browser based authentication bypass rule along with NTLM rule:

```
parameter-map type regex [parameter-map name]
pattern [pattern string]

ip admission name [rule name] ntlm
ip admission name [rule name] bypass regex [parameter-map name] absolute-timer
[absolute-time in minutes]
```

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

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

Authentication Failure

If a user fails authentication, the configured guest access policies are applied. The following are the causes of user authentication failures:

- Username, password, or both are incorrect in active NTLM authentication mode.
- Username is incorrect in passive NTLM authentication mode.
- LDAP server is not reachable. In this case, the user will not be asked to re-enter credentials as in other cases and there will be some time lag before ISR considers it as AAA Down case.

Default guest access is enabled by default. However, you can configure the maximum number of login attempts that are required before a user can fall back to the default guest access policy. The default 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 maximum login attempt value, configure the following command:

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

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

Authentication Failure and Watch-list behaviour

If a user fails authentication multiple times and max-login-attempts expire, that user is authenticated as a guest user and gets guest access. If watch-list is enabled as below:

ip admission watch-list enable

that user is added to the watch-list and the session state will be shown as SERVICE_DENIED. The user entry will be there in watch-list and the session state will remain in SERVICE_DENIED state for a default of 2 minutes, after which the session will be moved to the INIT state and the user will once again be prompted for credentials. Adjusting the time between authentication prompts can be adjusted by configuring the watch-list timeout as below:

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

For example, to ensure the user does not get re-prompted for credentials for 24 hours, configure the following:

ip admission watch-list expiry-time 1440

We recommend not to set the watch-list expiry timer to a very high value so that users are not prompted for credentials frequently. Setting zero (time of forever) is also not recommended as the user is never prompted for authentication and will not have granular user policies applied.

Domain and Non-Domain Users

Domain users who use transparent Windows NT Lan Manager (NTLM) authentication with supported browsers cannot login to the domain with invalid credentials. Because the device/domain will not let a user login 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 the password of a user expires, the user must log off and relogin to the domain with the new password.

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

The following users are considered as non-domain users:

- Domain users who do not use either Microsoft Internet Explorer or Google Chrome (These web browsers supports transparent NTLM by default.).
- A user who locally logs into a device (for example, workgroup machines that support local sign-on).
- Guest users

During authentication, non-domain users must specify the domain name (cisco\user1) and the password. If a user enters only the username and password, the client PC considers the hostname/computer name as the domain name and the user may not be authenticated, even when proper credentials were given.

For example, a corporate user User1 who uses a Mozilla Firefox web browser (that does not support transparent NTLM authentication by default) belongs to the “humanresources” domain. User1 must log into the domain with the username “humanresources\user1” to be recognized as a corporate user who has access to corporate policies configured on Cloud Web Security. If User1 logs in as just "user1", the user is authenticated as a guest user and only the default policy is applied.

IP HTTP Server and IP HTTP Secure-Server

When you enable the ip http server alone, HTTP requests will get intercepted for authentication and HTTPS request will pass through. Authentication that happens over HTTP is not secured. When you enable the ip http secure-server alone, HTTPS requests will get intercepted for authentication and HTTP requests will pass through. Authentication that happens over HTTPS is secured.

When you enable both ip http server and ip http secure-server, then both HTTP and HTTPS requests will get intercepted for authentication and authentication that happens over HTTPS and is secured. In this case, authentication happens over HTTPS even for HTTP requests.

Nested LDAP with NTLM Authentication

With this support, the LDAP client module can fetch both direct and nested user-group information for a user.

An LDAP search query retrieves the authorization profile of a user from an LDAP server to find direct user group members. Each of these direct user groups can be part of multiple groups and thus form a nested-user group.

Nested-level search will only occur within the base domain scope specified in the LDAP server configuration. 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 AD domain. Nested LDAP lookup requires a recursive search through the AD 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 AD depth of no more than 4-5 levels is recommended.

Perform the following task to enable nested LDAP search:

```
Device(config)# ldap server server1
Device(config-lap-server)# search-type nested
```

Configuration Examples

The following is a sample configuration on Cisco 4000 Series ISRs with NTLM authentication:

```
aaa new-model
!
aaa group server ldap cws-ldap-gr
 server cws-ldap
!
aaa authentication login default group ldap
aaa authentication login no-aaa none
aaa authorization network default group ldap
!
aaa session-id common
!
ip admission virtual-ip 2.2.2.2 virtual-host ciscoblr
ip admission watch-list enable
```

```
ip admission watch-list expiry-time 2
ip admission max-login-attempts 3
ip admission init-state-time 5
ip admission inactivity-timer 10
ip admission absolute-timer 200
ip admission name ntlm-active ntlm inactivity-time 20 absolute-timer 100 list allow_subnet
ip admission name ntlm-active bypass regex ua_bypass_pmap absolute-timer 10
ip admission name ntlm-passive ntlm passive inactivity-time 15 absolute-timer 100 list
deny_subnet
ip admission name ntlm-passive no-bypass regex ua_nobypass_pmap absolute-timer 10
!
parameter-map type regex ua_bypass_pmap
 pattern Safari
 pattern iTunes
!
parameter-map type regex ua_nobypass_pmap
 pattern Firefox
 pattern IE
 pattern Chrome
!
crypto pki trustpoint TP-self-signed-2995199412
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-2995199412
 revocation-check none
 rsakeypair TP-self-signed-2995199412
!
crypto pki certificate chain TP-self-signed-2995199412
 certificate self-signed 01
!
interface GigabitEthernet0/0/0
 ip address 181.168.1.50 255.255.0.0
 ip admission ntlm-active
!
interface GigabitEthernet0/0/1
 ip address 183.168.1.50 255.255.255.0
!
ip http server
ip http secure-server
!
ip access-list extended allow_subnet
 permit ip 181.168.1.0 0.255.255.255 183.168.1.0 0.0.0.255
!
ip access-list extended deny_subnet
 deny ip host 181.168.1.20 any
 permit ip any any
!
ldap server cws-ldap
 ipv4 183.168.1.5
 base-dn cn=users,dc=xsa,dc=cisco,dc=com
 search-type nested
 search-filter user-object-type top
 authentication bind-first
!
line con 0
 exec-timeout 0 0
 login authentication no-aaa
!
```

The following example shows how to display ip admission cache information:

```
show ip admission cache
```

```
Authentication Proxy Cache
Legend:
  ^ - Sleeping Client
Total Sessions: 2 Init Sessions: 1
 Client MAC 0000.0000.0000 Client IP 181.168.1.7 IPv6 ::, State AUTHZ, Method NTLM
 Client MAC 0000.0000.0000 Client IP 181.168.1.6 IPv6 ::, State INIT, Method NTLM
 Client MAC 0000.0000.0000 Client IP 181.168.1.5 IPv6 ::, State ESTAB (Browser bypass),
Method NTLM
 Client MAC 0000.0000.0000 Client IP 181.168.1.9 IPv6 ::, State AUTHC_FAIL[AAA DOWN],
Method NTLM
 Client MAC 0000.0000.0000 Client IP 181.168.1.8 IPv6 ::, State AUTHC_FAIL[INVALID
CREDENTIALS], Method NTLM
 Client MAC 0000.0000.0000 Client IP 181.168.1.10 IPv6 ::, State SERVICE_DENIED, Method
NTLM
```

The following example shows how to display ip admission detail information for a particular client session:

```
show authentication session ip 191.168.1.7 details
            Interface:  GigabitEthernet0/0/0
          MAC Address:  Unknown
         IPv6 Address:  Unknown
         IPv4 Address:  181.168.1.7
            User-Name:  cwsuser
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  000000000000000150066E8B9
      Acct Session ID:  Unknown
               Handle:  0x3F000009
       Current Policy:  POLICY_Gi0/0/0

User-group(s):
    cwsug3, cwsug2, cwsug1

Local Policies:
    Service Template: webauth-global-inactive (priority 150)
         Idle timeout:  3600 sec
    Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Method status list:
       Method           State
       webauth          Authc Success
```

Additional References

Related Documents

Related Topic	Document Title
Security commands: complete command syntax, command mode, command history, defaults, usage guidelines, and examples.	*Cisco IOS Security command reference guides*.
Cisco IOS Commands	*Cisco IOS Master Commands List, All Releases*

Standards

Standards	Title
None	—

MIBs

MIBs	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases and feature sets, use Cisco MIB locator http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	—

Technical Assistance

Description	Title
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for NTLM Authentication on the Cisco 4000 Series ISR

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator www.cisco.com/go/cfn to find information about platform support and Cisco software image support. An account on Cisco.com is not required.

Table 1 Feature Information for NTLM Authentication on the Cisco 4000 Series ISR

Feature Name	Releases	Feature Information
NTLM Authentication on the Cisco 4000 Series ISR	Cisco XE 3.17	NTLM Authentication on Cisco 4000 Series ISRs. The Cisco 4000 Series ISRs with NTLM Authentication and Cloud Web Security solution can enable branch offices to intelligently redirect web traffic to the cloud to enforce granular security policies over user web traffic.