直通和直接ASA身份驗證配置示例

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[慣例](#)
[直通](#)
[直接驗證](#)

簡介

本文檔介紹如何配置直通和直接ASA身份驗證。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據思科調適型安全裝置(ASA)。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

如需文件慣例的詳細資訊，請參閱[思科技術提示慣例。](#)

直通

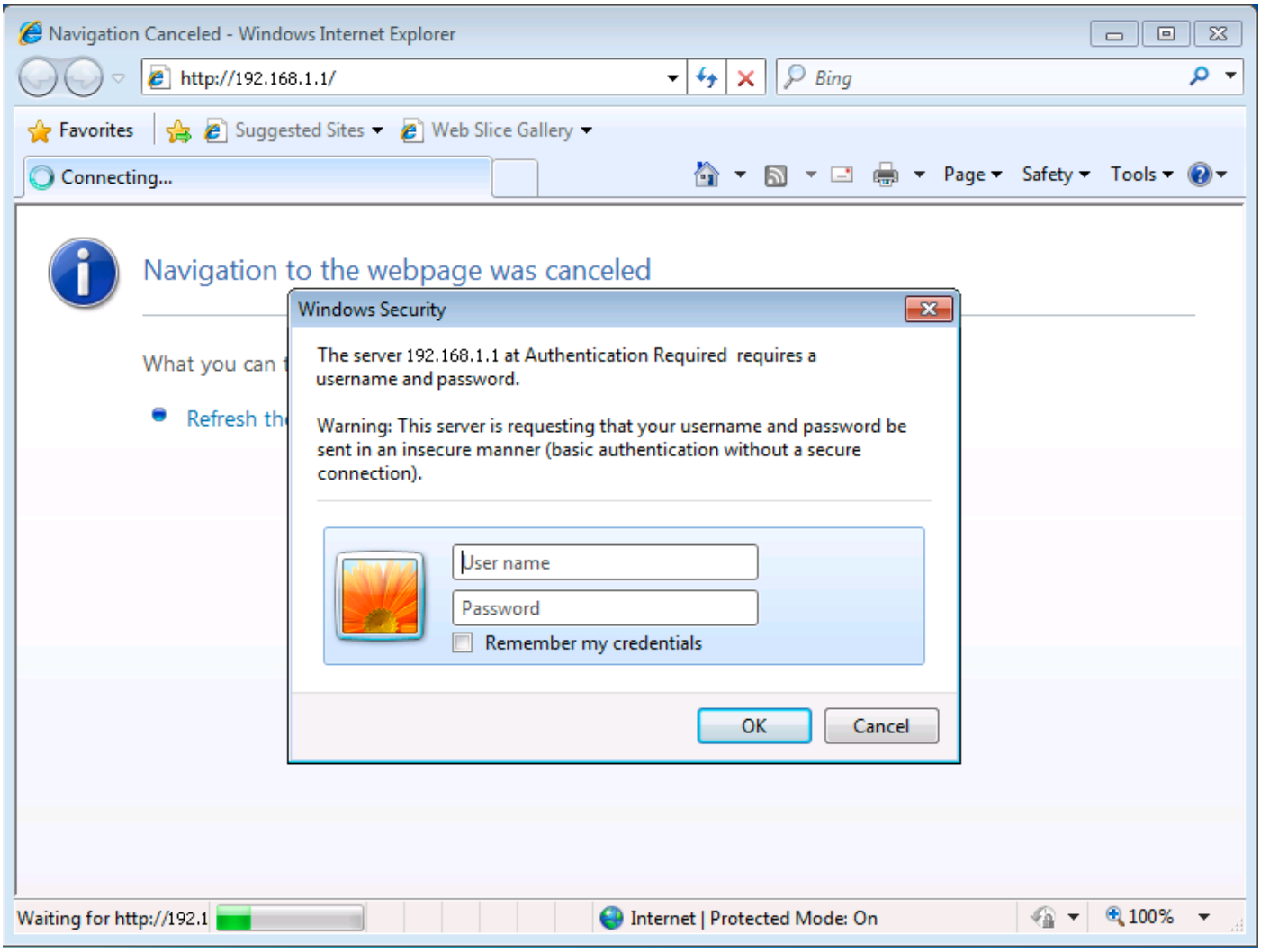
直通身份驗證之前使用aaa authentication include**命令進行**配置。現在使用**aaa authentication match**命令。需要身份驗證的流量在**aaa authentication match**命令引用的訪問清單中允許，這會導致主機在允許指定流量通過ASA之前進行身份驗證。

以下是Web流量驗證的組態範例：

```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 80
aaa authentication match authmatch inside LOCAL
```

請注意，此解決方案之所以起作用，是因為HTTP是一種協定，ASA可以在其中注入身份驗證。

ASA會攔截HTTP流量並通過HTTP身份驗證對其進行身份驗證。由於身份驗證是以內嵌方式注入的，因此Web瀏覽器中會出現一個HTTP身份驗證對話方塊，如下圖所示：



直接驗證

直接身份驗證以前使用**aaa authentication include**和**virtual <protocol>**命令配置。現在，使用**aaa authentication match**和**aaa authentication listener**命令。

對於本地不支援身份驗證的協定（即無法內聯身份驗證質詢的協定），可以配置直接ASA身份驗證。預設情況下，ASA不偵聽身份驗證請求。可以使用**aaa authentication listener**命令在特定埠和介面上配置監聽程式。

以下是主機通過驗證後允許TCP/3389流量通過ASA的配置示例：

```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 3389
access-list authmatch permit tcp any host 10.245.112.1 eq 5555
aaa authentication match authmatch inside LOCAL
aaa authentication listener http inside port 5555
```

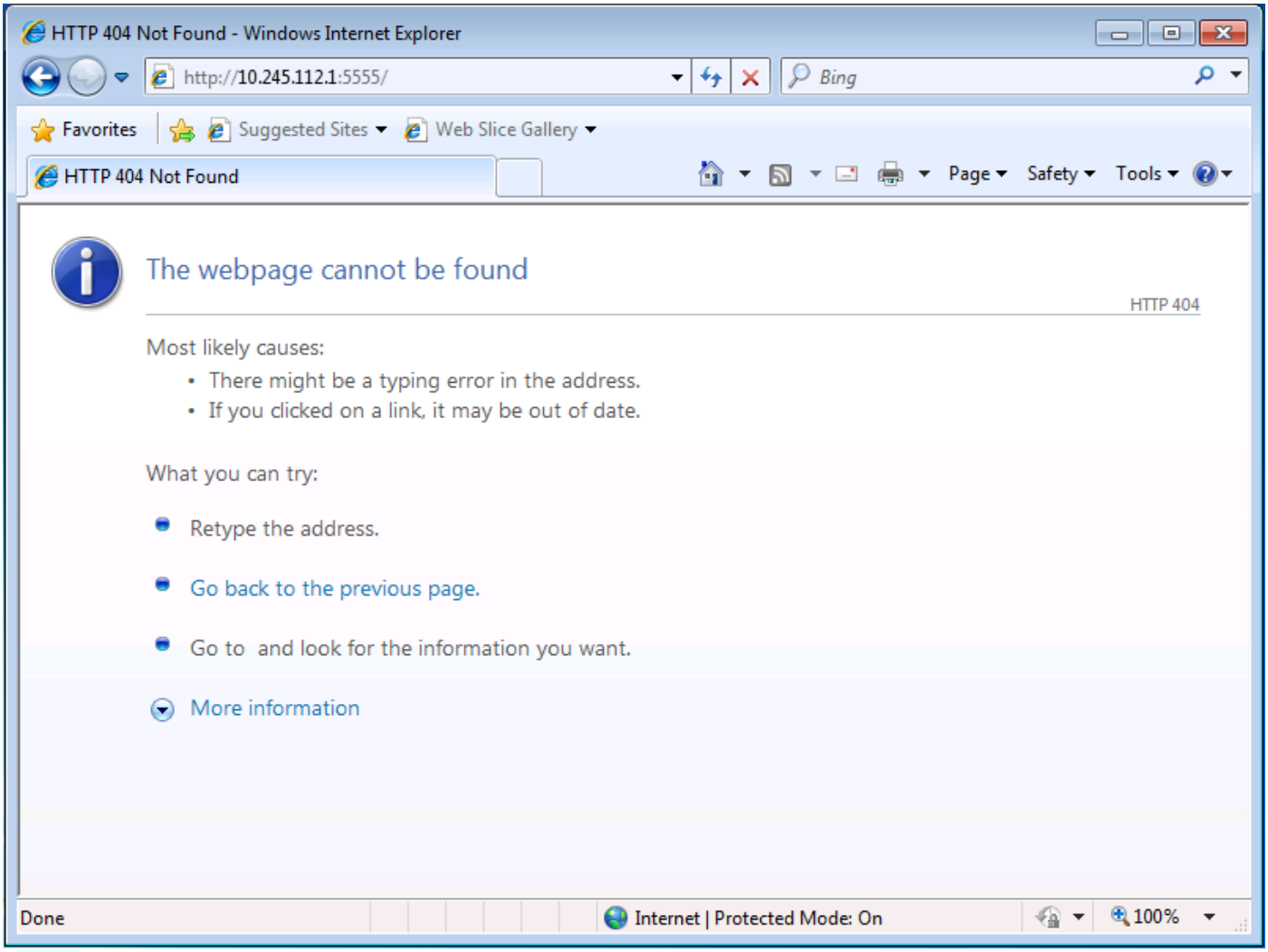
記下監聽程式使用的埠號(TCP/5555)。 **show asp table socket**命令輸出顯示，ASA現在在分配給指定（內部）介面的IP地址處監聽對此埠的連線請求。

```
ciscoasa(config)# show asp table socket
```

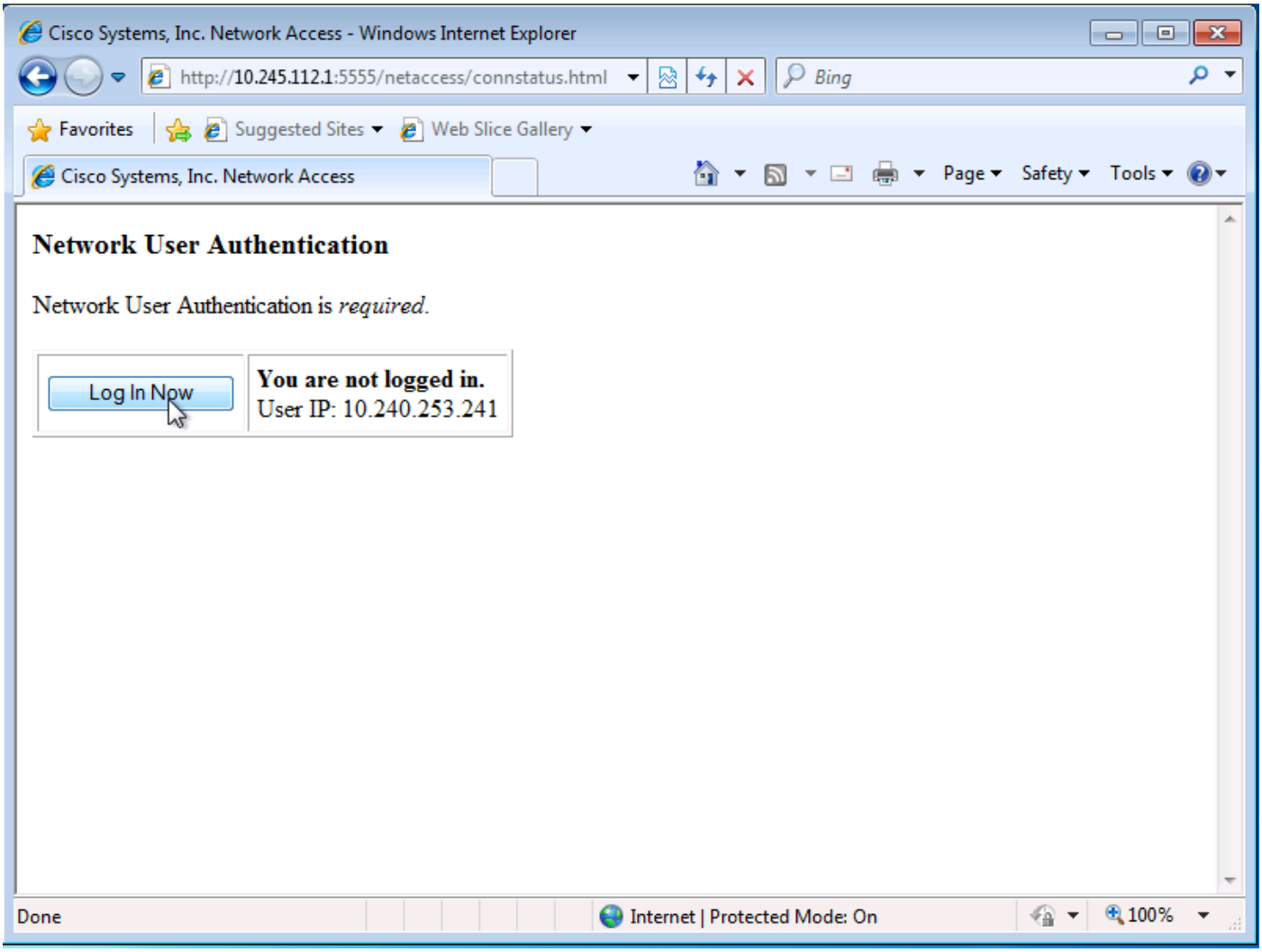
```
Protocol Socket Local Address Foreign Address State
TCP 000574cf 10.245.112.1:5555 0.0.0.0:* LISTEN
ciscoasa(config)#
```

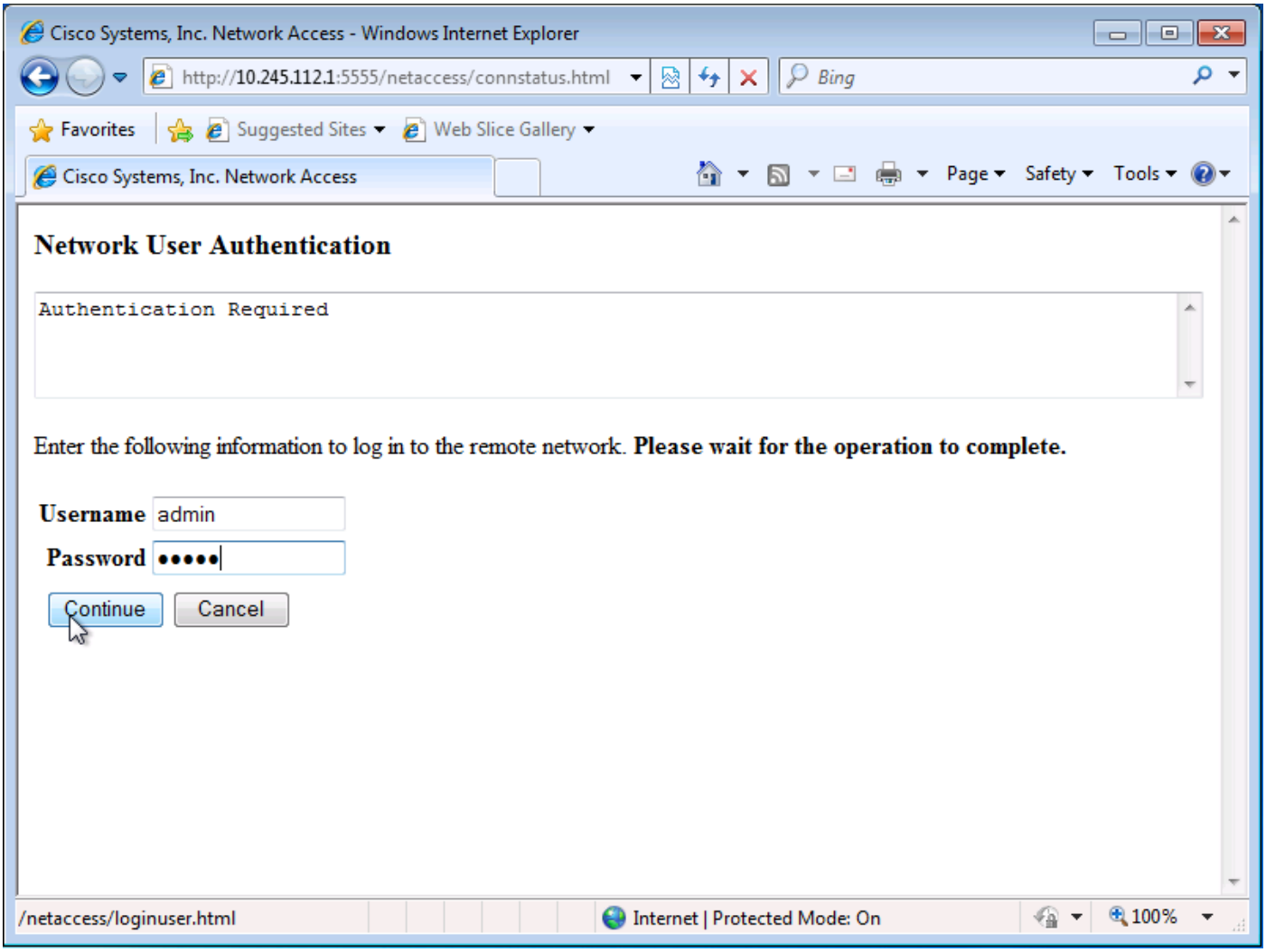
按照如上所示配置ASA後，通過ASA嘗試連線到TCP埠3389上的外部主機將導致拒絕連線。使用者必須先進行身份驗證，才能允許TCP/3389流量。

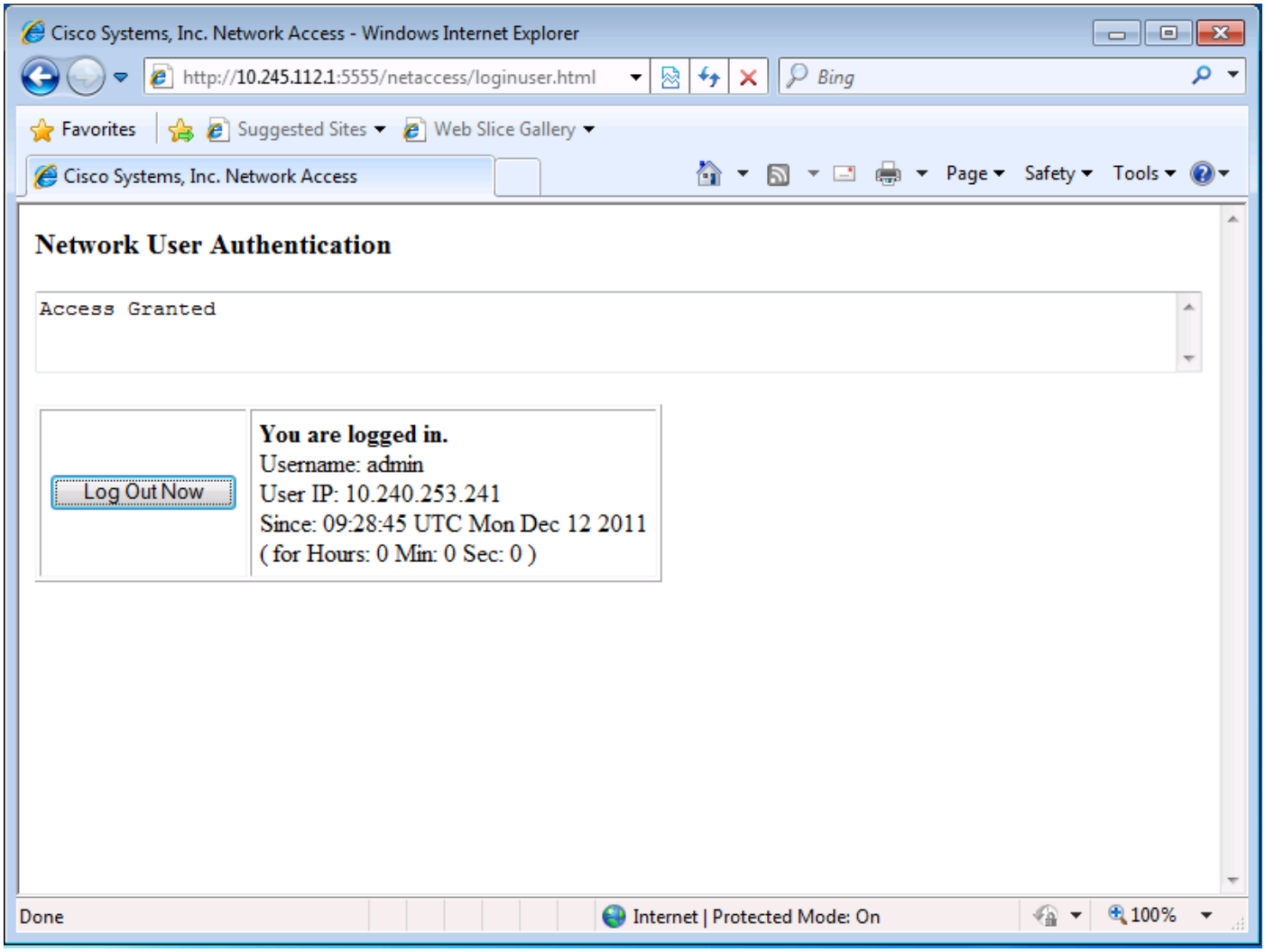
直接身份驗證要求使用者直接瀏覽到ASA。如果瀏覽到http://<*asa_ip*>:<*port*>，將返回404錯誤，因為ASA Web伺服器的根目錄上不存在網頁。



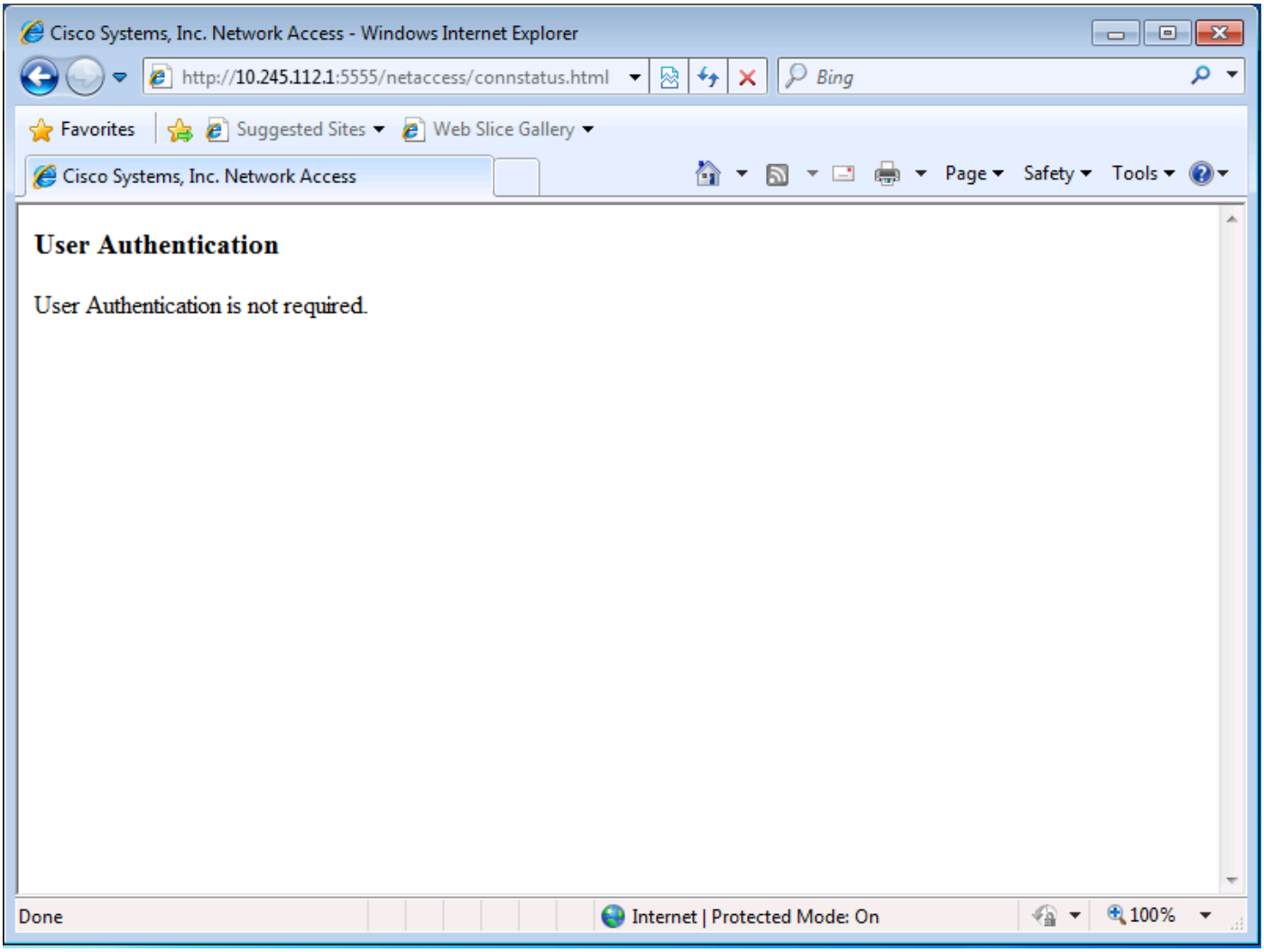
您必須直接瀏覽到http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html。登入頁面位於此URL，您可以在其中提供驗證憑證。


Cisco Systems, Inc. Network Access - Windows Internet Explorer
http://10.245.112.1:5555/netaccess/connstatus.html
Bing
Favorites
Suggested Sites
Web Slice Gallery
Cisco Systems, Inc. Network Access
Page
Safety
Tools
Network User Authentication
Network User Authentication is required.
Log In Now
You are not logged in.
User IP: 10.240.253.241
Done
Internet | Protected Mode: On
100%


Cisco Systems, Inc. Network Access - Windows Internet Explorer
http://10.245.112.1:5555/netaccess/connstatus.html
Bing
Favorites
Suggested Sites
Web Slice Gallery
Cisco Systems, Inc. Network Access
Page
Safety
Tools
Network User Authentication
Authentication Required
Enter the following information to log in to the remote network. Please wait for the operation to complete.
Username
admin
Password
Continue
Cancel
/netaccess/loginuser.html
Internet | Protected Mode: On
100%



在此配置中，直接身份驗證流量是authmatch access-list的一部分。如果缺少此訪問控制項，當您瀏覽到http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html時，可能會收到意外消息，例如*User Authentication， User Authentication is not required。*



成功進行身份驗證後，可以通過ASA連線到TCP/3389上的外部伺服器。