Cut-Through and Direct ASA Authentication Configuration Example

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Components Used](#)
[Conventions](#)
[Cut-Through](#)
[Direct Authentication](#)

Introduction

This document describes how to configure cut-through and direct ASA authentication.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on the Cisco Adaptive Security Appliance (ASA).

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

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

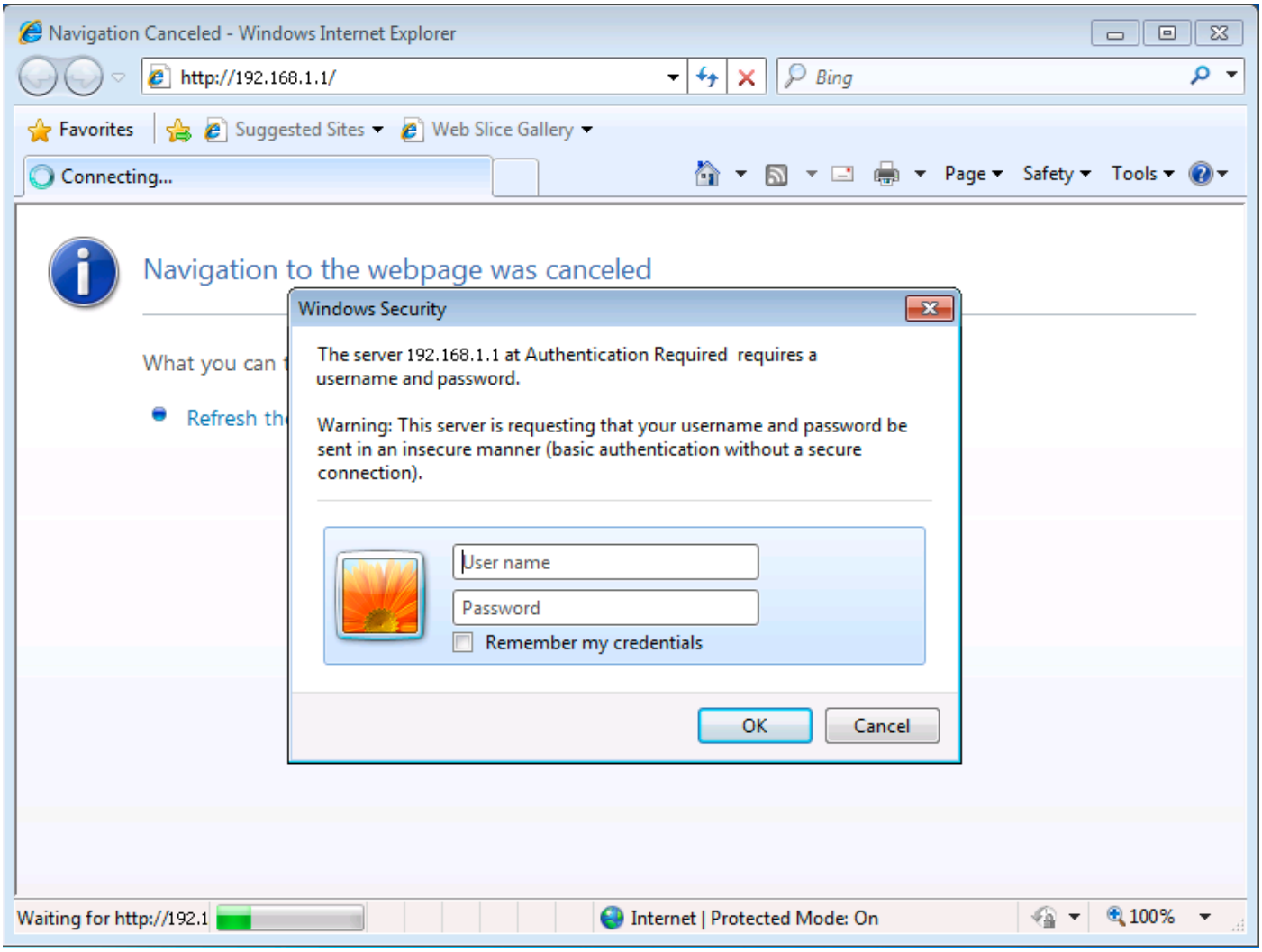
Cut-Through

Cut-through authentication was previously configured with the **aaa authentication include** command. Now, the **aaa authentication match** command is used. Traffic that requires authentication is permitted in an access list that is referenced by the **aaa authentication match** command, which causes the host to be authenticated before the specified traffic is allowed through the ASA.

Here is a configuration example for web traffic authentication:

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

Note that this solution works because HTTP is a protocol in which the ASA can inject authentication. The ASA intercepts HTTP traffic and authenticates it via HTTP authentication. Because the authentication is injected inline, an HTTP authentication dialog box appears in the web browser as shown in this image:



Direct Authentication

Direct authentication was previously configured with the **aaa authentication include** and **virtual < protocol>** commands. Now, the **aaa authentication match** and **aaa authentication listener** commands are used.

For protocols that do not support authentication natively (that is, protocols that cannot have an authentication challenge inline), direct ASA authentication can be configured. By default, the ASA does not listen for authentication requests. A listener can be configured on a particular port and interface with the **aaa authentication listener** command.

Here is a configuration example that allows TCP/3389 traffic through the ASA once a host has been authenticated:

```
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
```

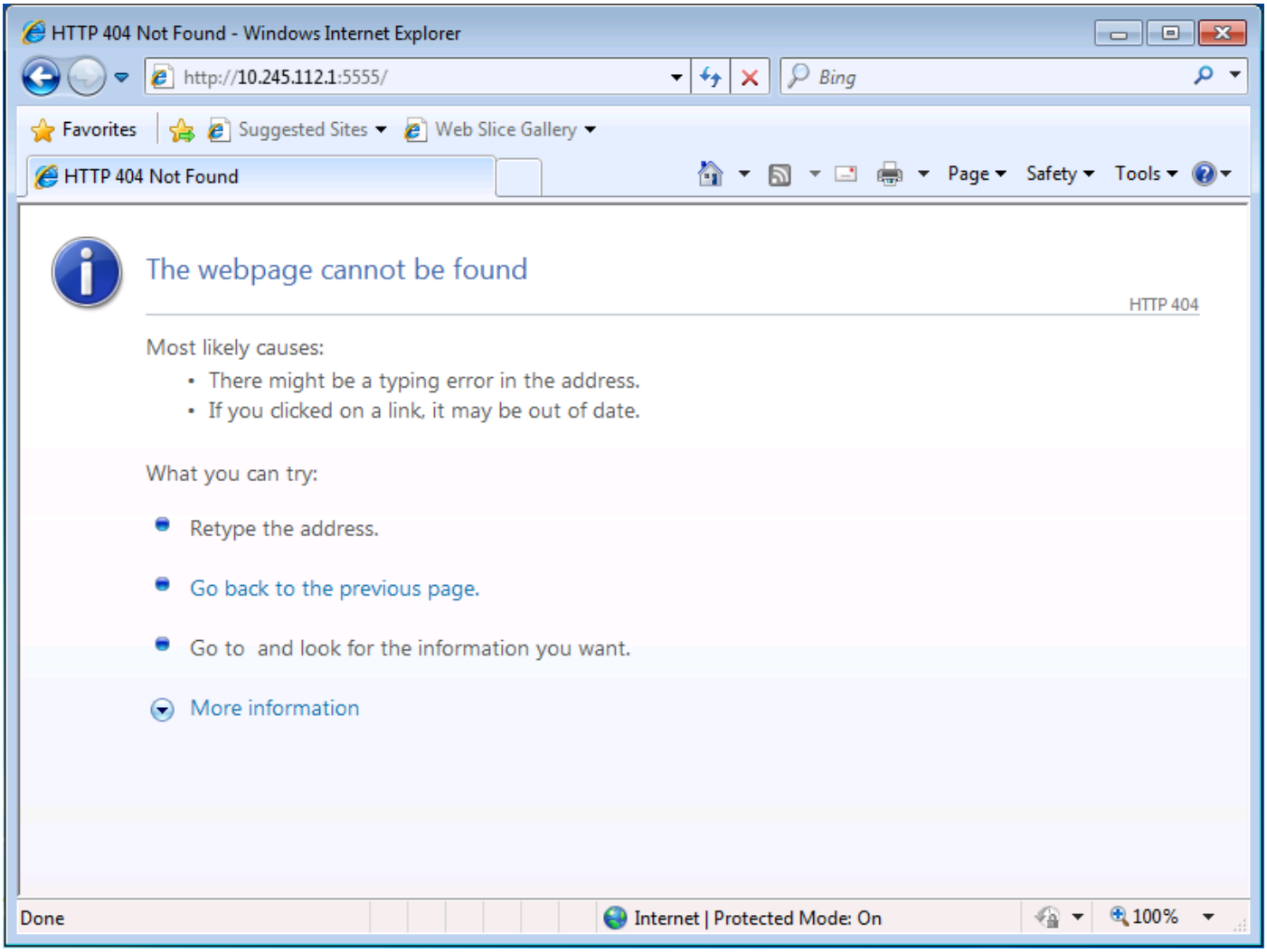
Note the port number that is used by the listener (TCP/5555). The **show asp table socket** command output shows that the ASA now listens for connection requests to this port at the IP address assigned to the specified (inside) interface.

```
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)#
```

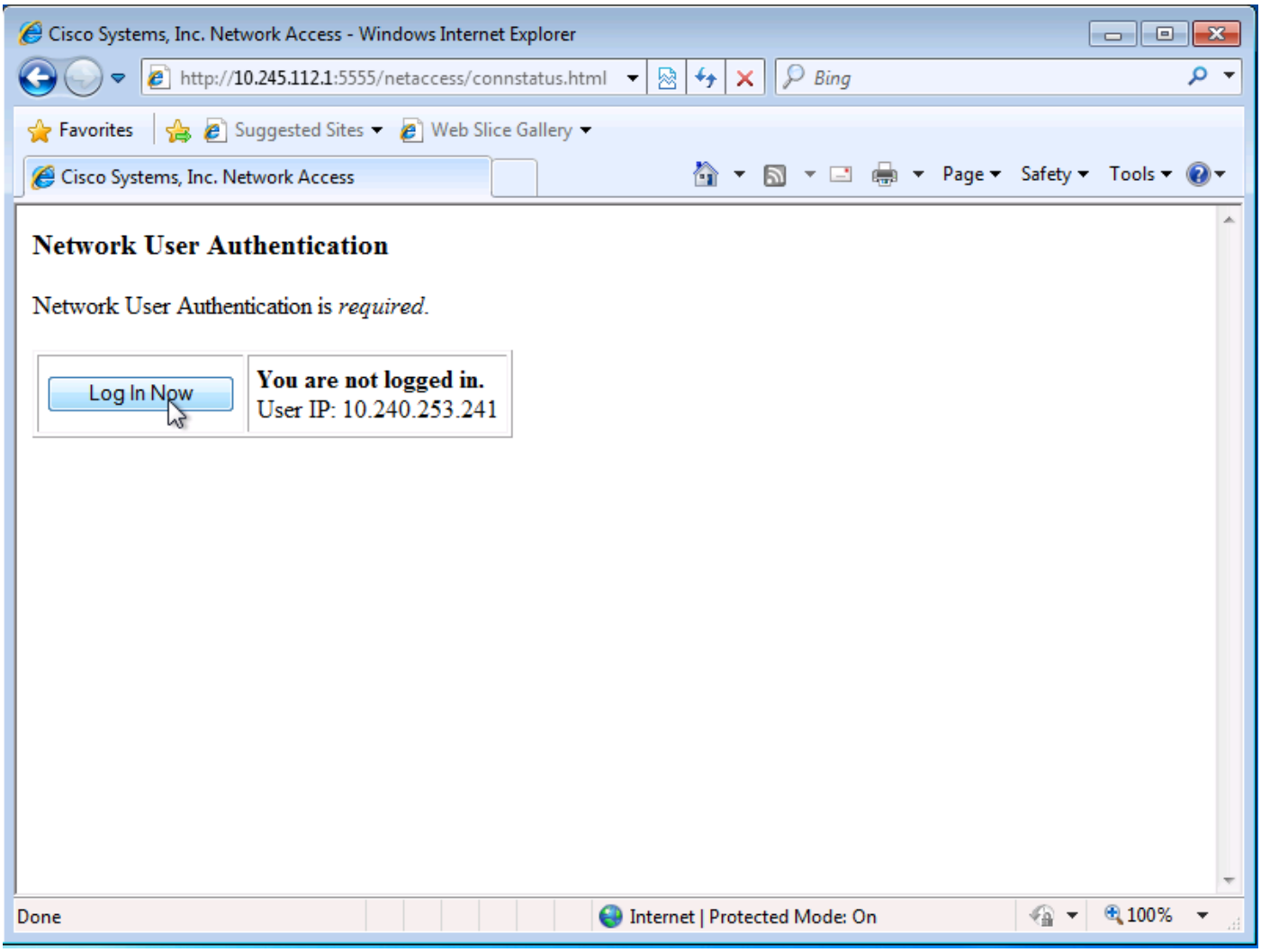
After the ASA is configured as shown above, a connection attempt through the ASA to an outside host on TCP port 3389 will result in a connection denial. The user must first authenticate for TCP/3389 traffic to be allowed.

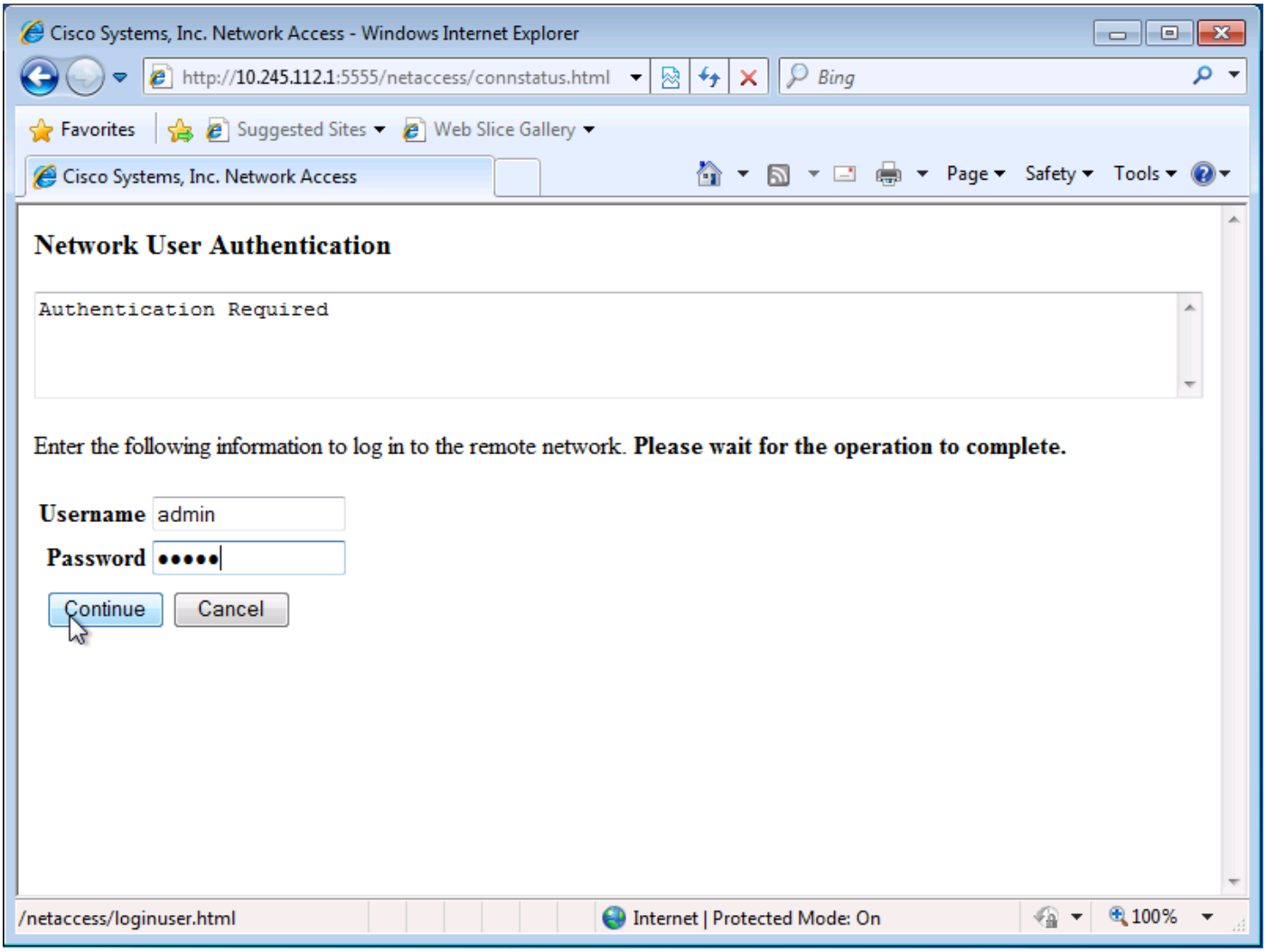
Direct authentication requires the user to browse directly to the ASA. If you browse to http://<*asa_ip*>:<*port*>, a 404 error is returned because no web page exists at the root of the ASA's web server.

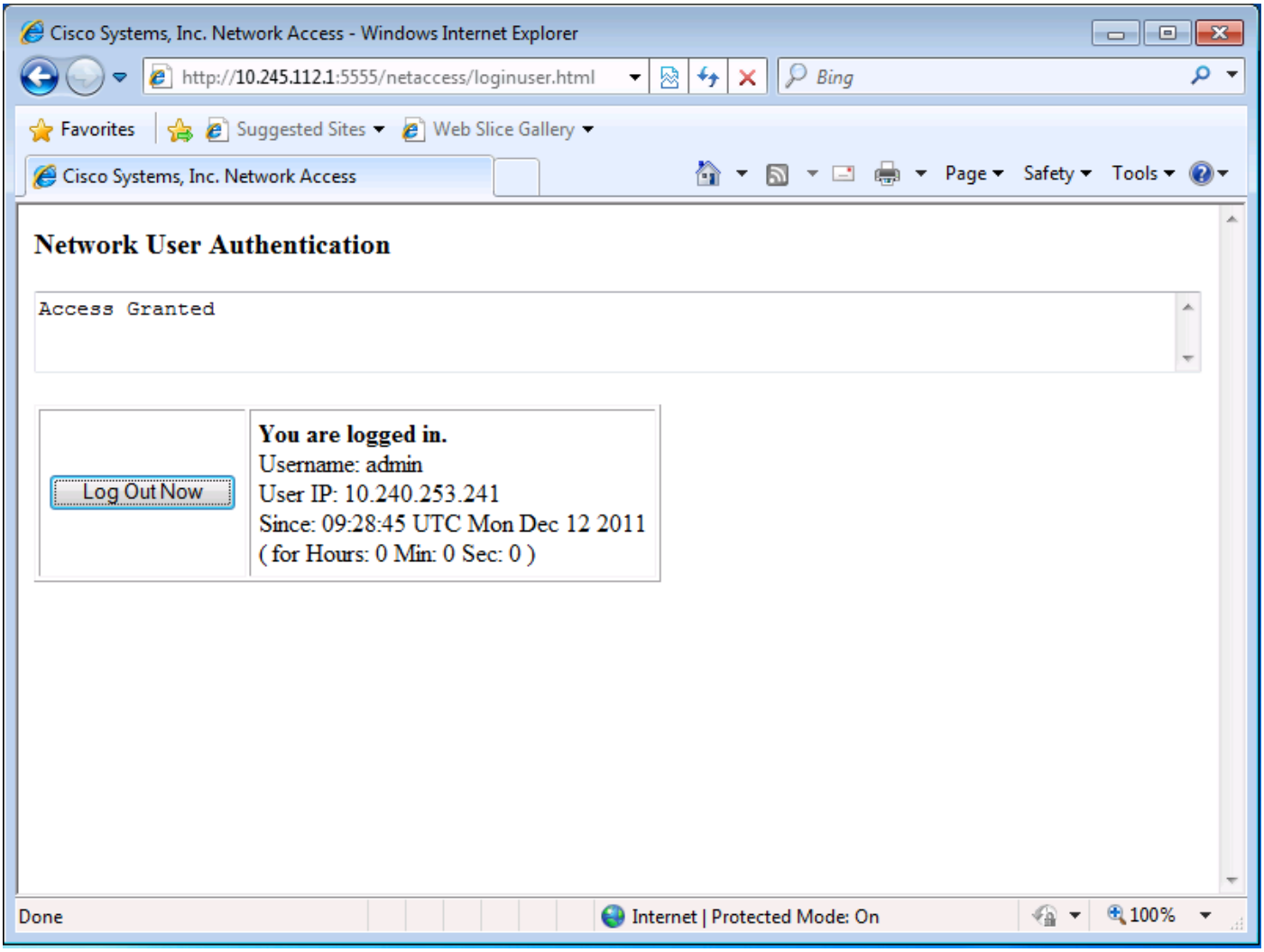


Instead, you must browse directly to http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html. A

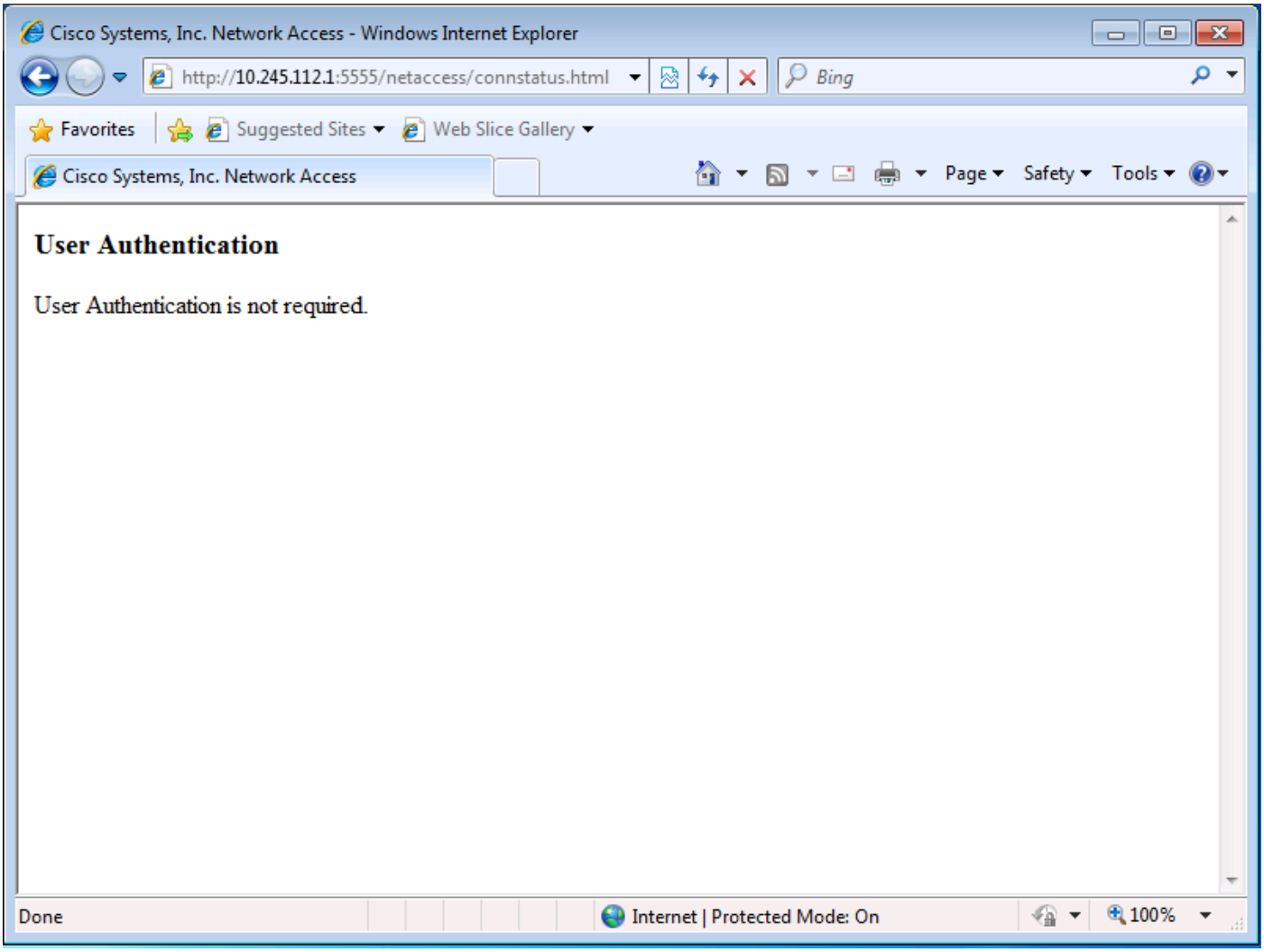
login page resides at this URL where you can provide authentication credentials.




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%



In this configuration, the direct authentication traffic is part of the authmatch access-list. Without this access-control entry, you might receive an unexpected message, such as *User Authentication, User Authentication is not required,* when you browse to http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html.



After you authenticate successfully, you can connect through the ASA to an outside server on TCP/3389.