直通和直接ASA身份验证配置示例

目录

简介

本文档介绍如何配置直通和直接ASA身份验证。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于思科自适应安全设备(ASA)。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

直通

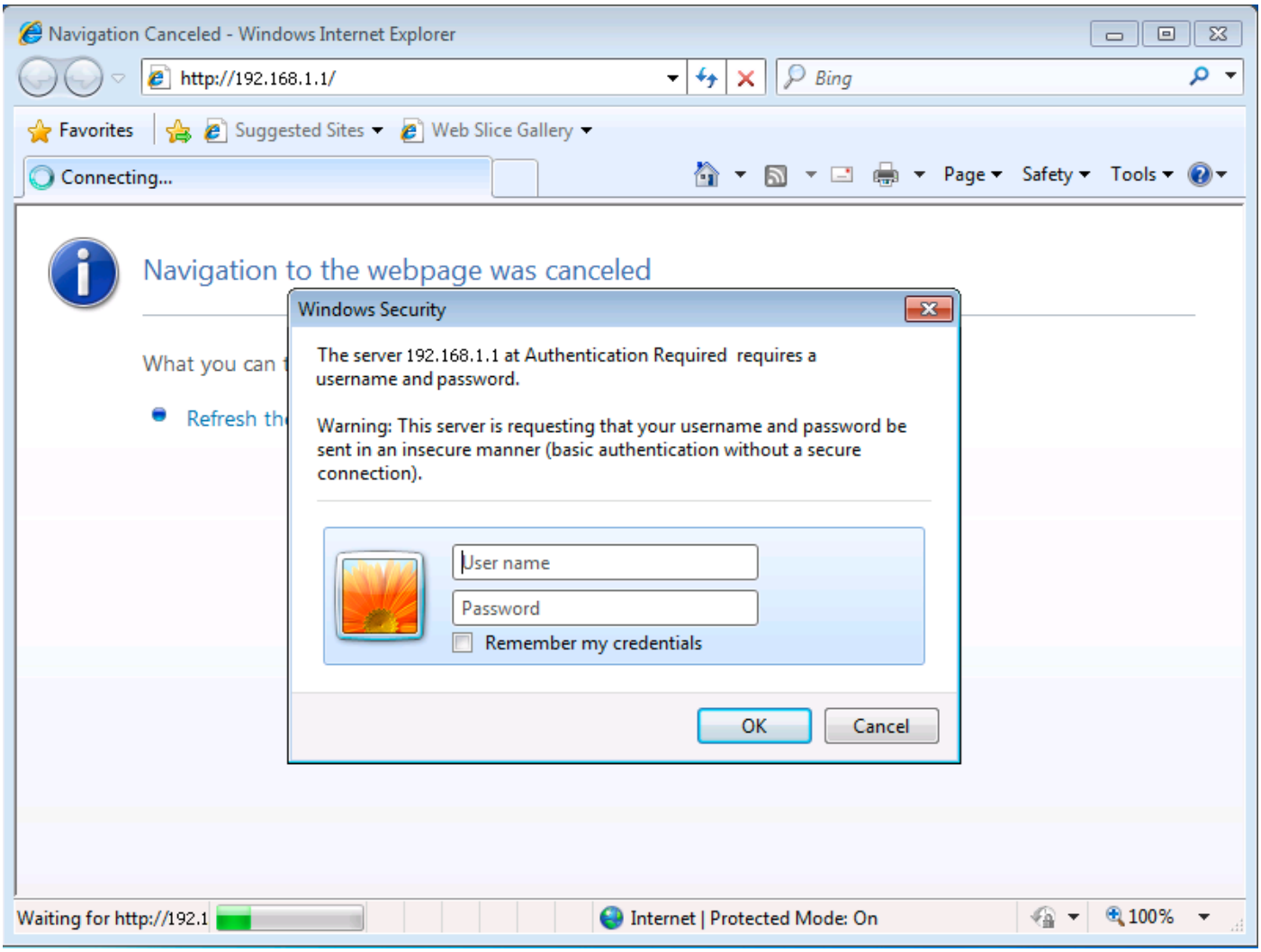
之前使用aaa authentication include命令配置了直通**身份验证。**现在，使**用aaa authentication** match命令。需要身份验证的流量允许在**aaa authentication match**命令引用的访问列表中，这会导致主机在指定流量允许通过ASA之前进行身份验证。

以下是Web流量身份验证的配置示例：

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

请注意，此解决方案之所以有效，是因为HTTP是ASA可以注入身份验证的协议。ASA拦截HTTP流

量并通过HTTP身份验证对其进行身份验证。由于身份验证是内联注入的，因此Web浏览器中会显示HTTP身份验证对话框，如下图所示：



直接身份验证

之前使用aaa authentication include和virtual **<protocol>命令配置了直接身**份验证。现在，使**用aaa authentication match和aaa authentication listener**命令。

对于本地不支持身份验证的协议（即不能内联身份验证质询的协议），可以配置直接ASA身份验证。默认情况下，ASA不侦听身份验证请求。可以使用aaa authentication listener命令在特定端口和接口上**配置侦听**程序。

以下是允许TCP/3389流量在主机经过身份验证后通过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
```

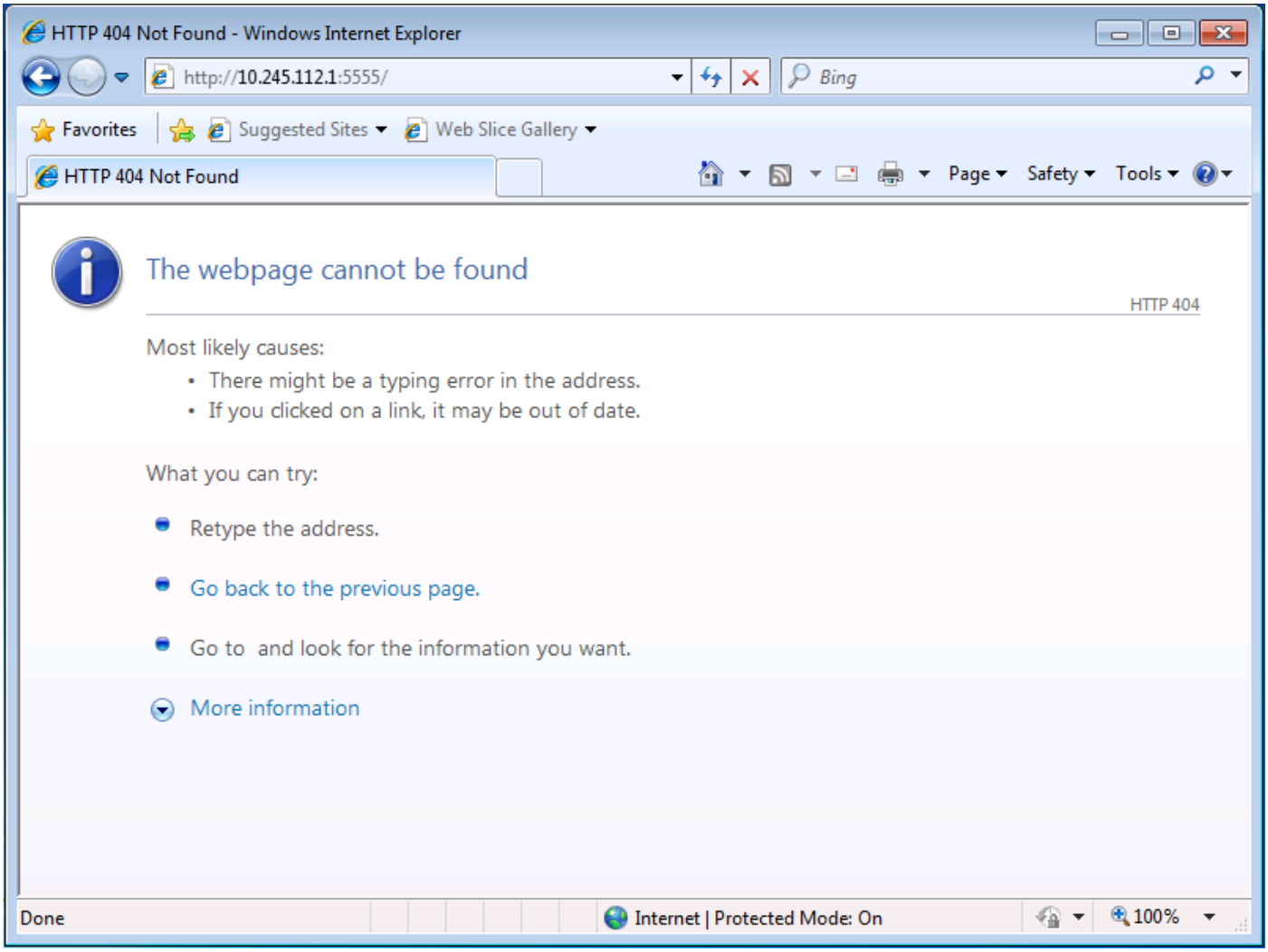
注意侦听程序使用的端口号(TCP/5555)。 **show asp table socket**命令输出显示，ASA现在侦听到此端口的连接请求，该端口的IP地址已分配给指定（内部）接口。

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

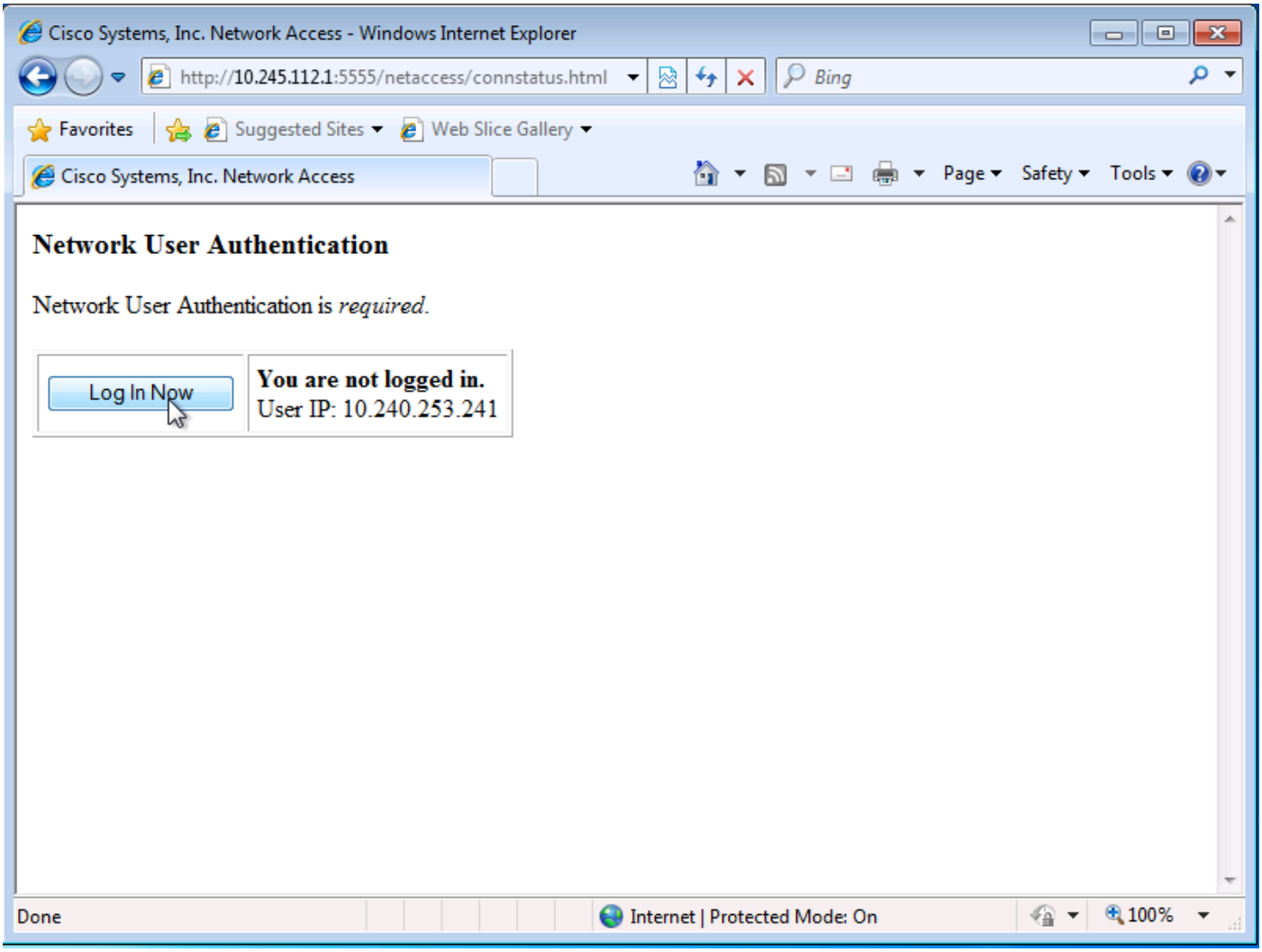
```
Protocol Socket Local Address Foreign Address State
TCP 000574cf 10.245.112.1:5555 0.0.0.0:* LISTEN
ciscoasa(config)#
```

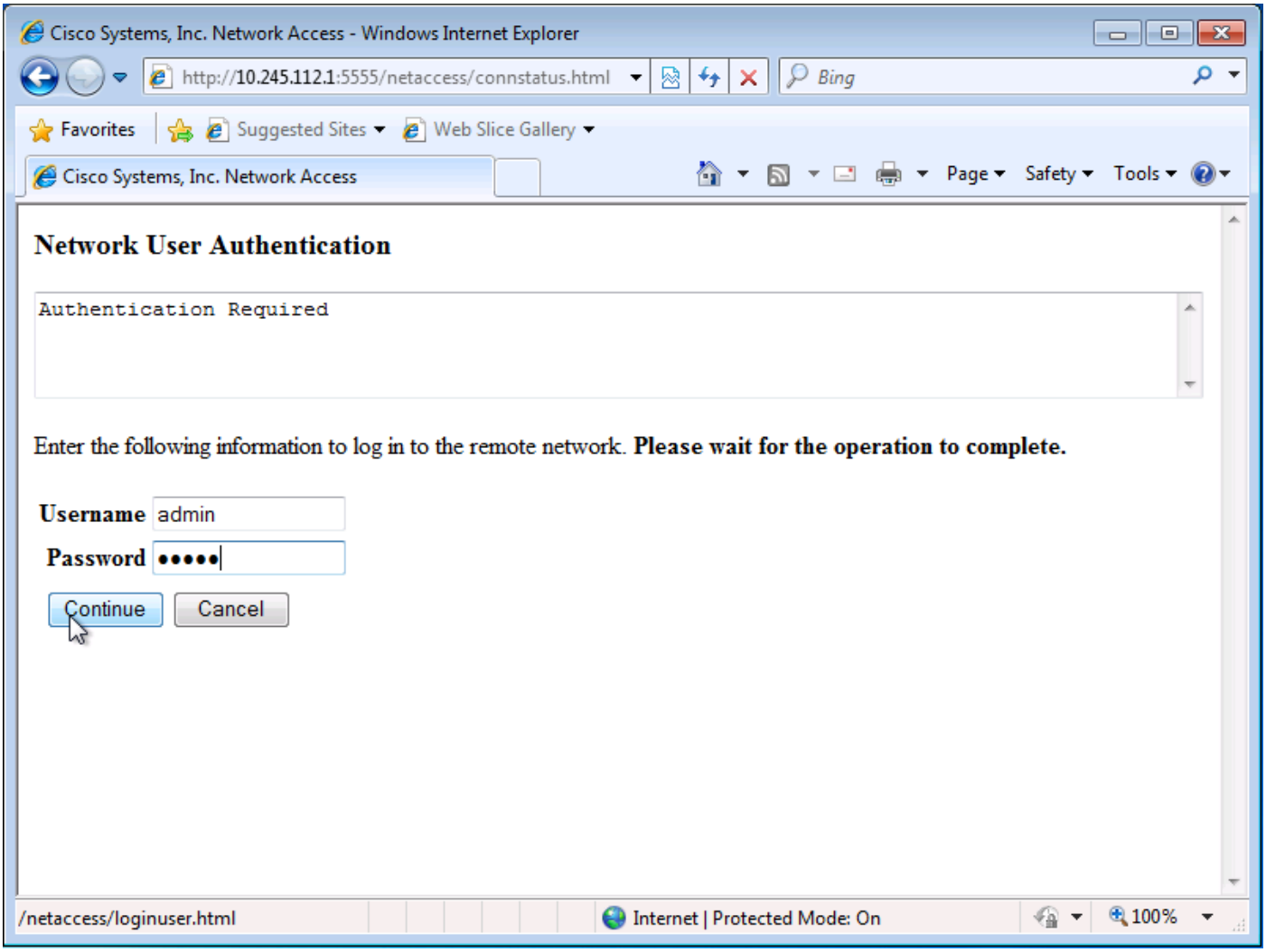
如上所示配置ASA后，通过ASA连接到TCP端口3389上的外部主机的尝试将导致连接拒绝。用户必须首先对允许的TCP/3389流量进行身份验证。

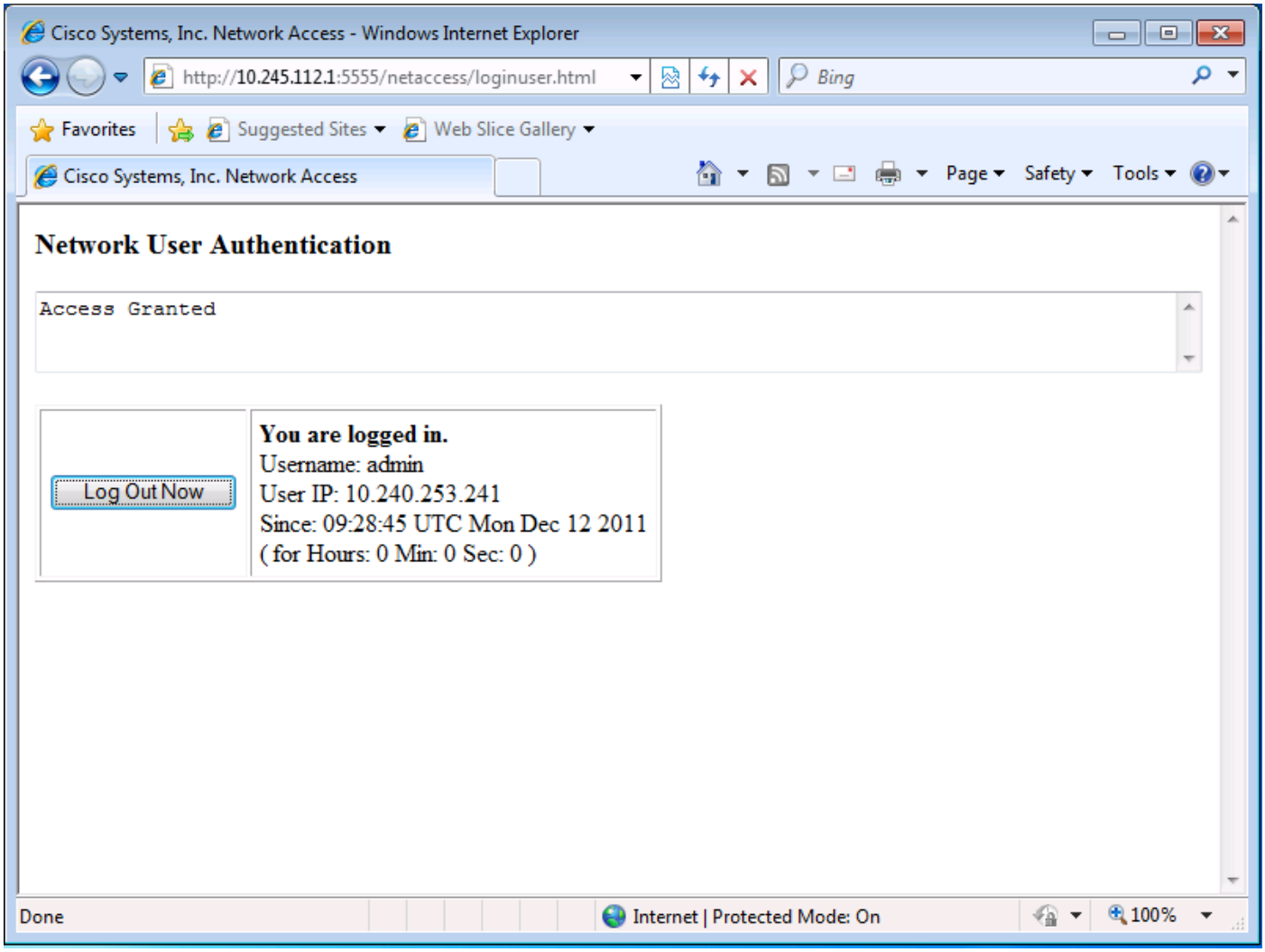
直接身份验证要求用户直接浏览ASA。如果浏览到http://<*asa_ip*>:<*port*>，则返回404错误，因为ASA Web服务器的根上不存在任何网页。



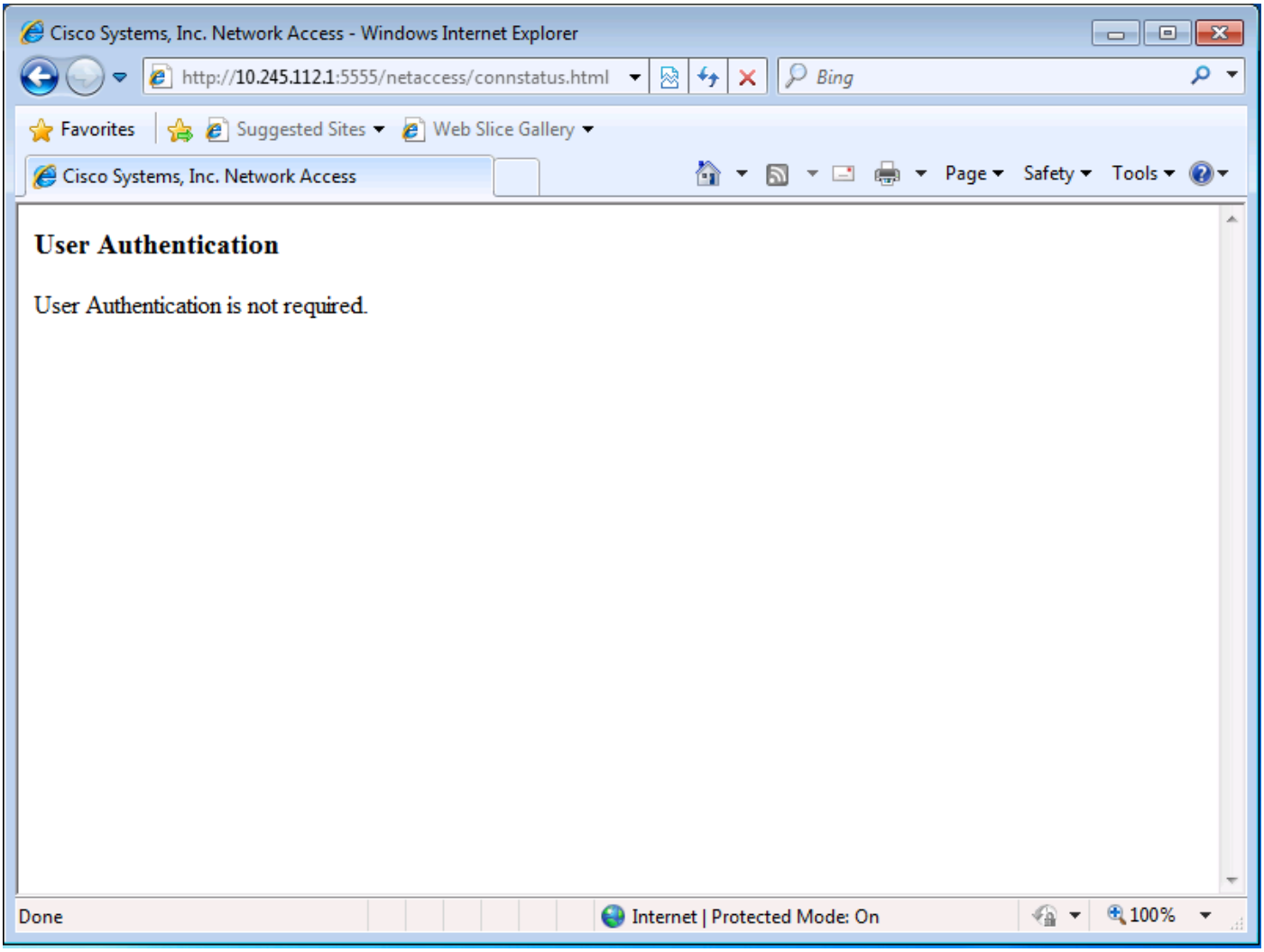
相反，您必须直接浏览到http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html。登录页位于此URL上，您可以在此URL上提供身份验证凭证。


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，直接身份验证流量是authmatch access-list的一部分。如果没有此访问控制条目，当您浏览到http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html时，可能会收到意外消息，如*User Authentication*， *User Authentication is not required*。



成功进行身份验证后，可以通过ASA连接到TCP/3389上的外部服务器。