Ejemplo de Configuración de Autenticación ASA Directa y de Corte

Contenido

Introducción

Este documento describe cómo configurar la autenticación ASA directa y cut-through.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en el dispositivo de seguridad adaptable (ASA) de Cisco.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

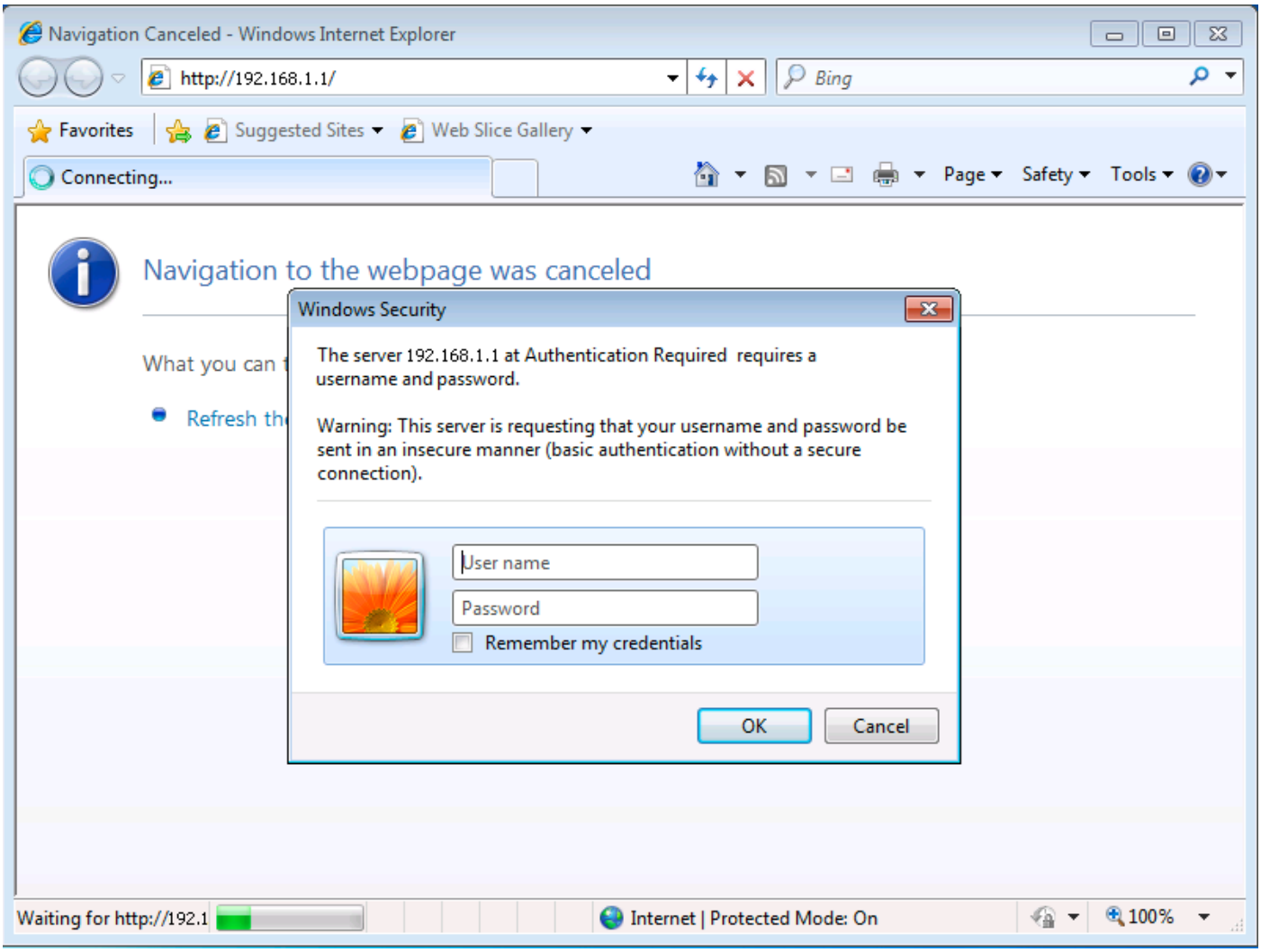
Corte-por

La autenticación de acceso directo se configuró previamente con el comando **aaa authentication include**. Ahora, se utiliza el comando **aaa authentication match**. El tráfico que requiere autenticación se permite en una lista de acceso a la que hace referencia el comando **aaa authentication match**, que hace que el host se autentique antes de que se permita el tráfico especificado a través del ASA.

Este es un ejemplo de configuración para la autenticación del tráfico web:

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

Tenga en cuenta que esta solución funciona porque HTTP es un protocolo en el que ASA puede inyectar autenticación. El ASA intercepta el tráfico HTTP y lo autentica a través de la autenticación HTTP. Debido a que la autenticación se inserta en línea, aparece un cuadro de diálogo de autenticación HTTP en el navegador web como se muestra en esta imagen:



Autenticación directa

La autenticación directa se configuró previamente con los comandos **aaa authentication include** y **virtual < protocol>**. Ahora, se utilizan los comandos **aaa authentication match** y **aaa authentication listener**.

Para los protocolos que no admiten la autenticación nativa (es decir, los protocolos que no pueden tener un desafío de autenticación en línea), se puede configurar la autenticación ASA directa. De forma predeterminada, el ASA no escucha las solicitudes de autenticación. Un listener se puede configurar en un puerto determinado y en la interfaz con el comando **aaa authentication listener**.

Este es un ejemplo de configuración que permite el tráfico TCP/3389 a través del ASA una vez

que se ha autenticado un host:

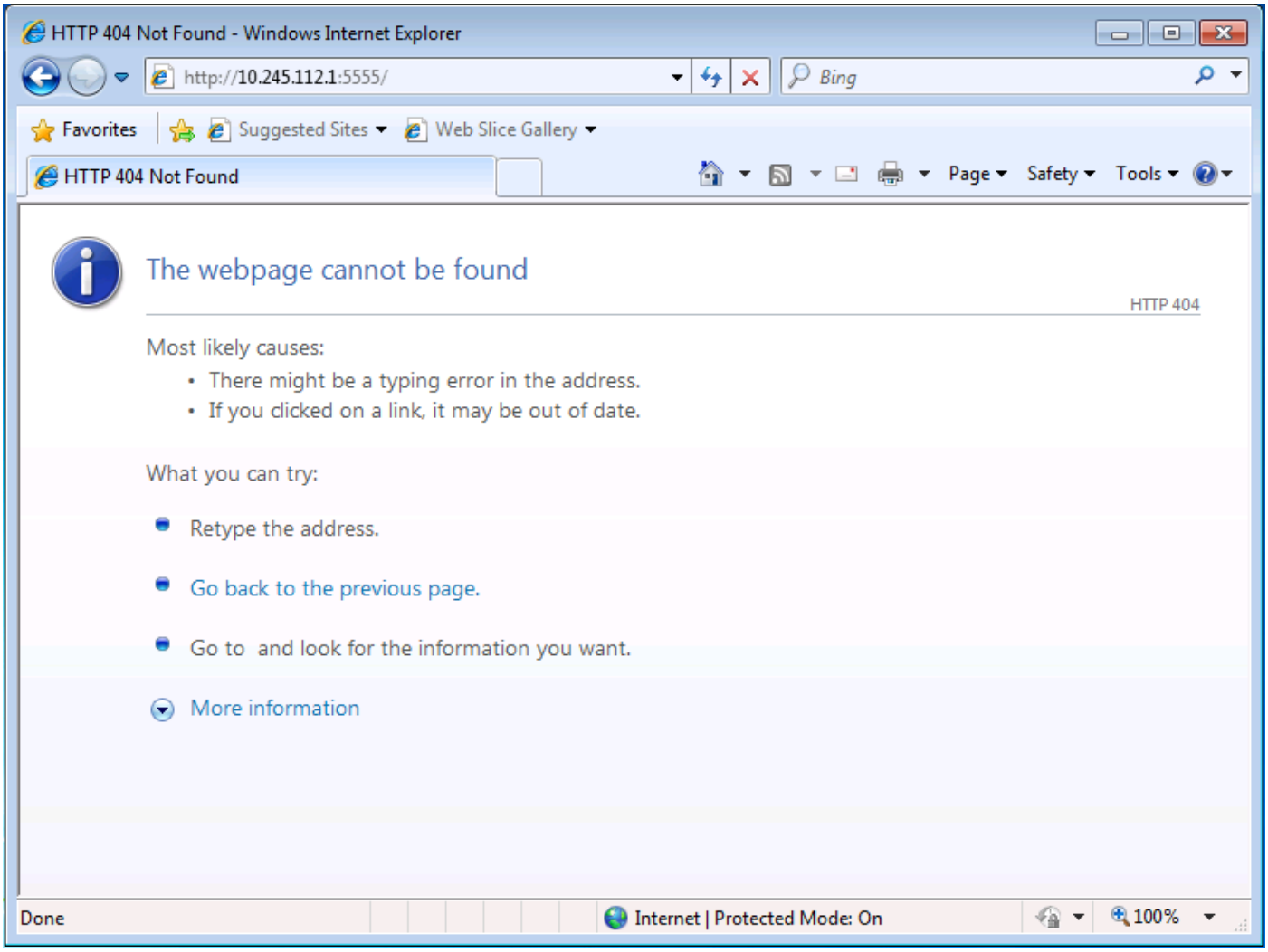
```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 3389
access-list authmatch permit tcp any host 10.245.112.1 eq 5555
aaa authentication match authmatch inside LOCAL
aaa authentication listener http inside port 5555
```

Observe el número de puerto que utiliza el receptor (TCP/5555). La salida del comando **show asp table socket** muestra que el ASA ahora escucha las solicitudes de conexión a este puerto en la dirección IP asignada a la interfaz especificada (interna).

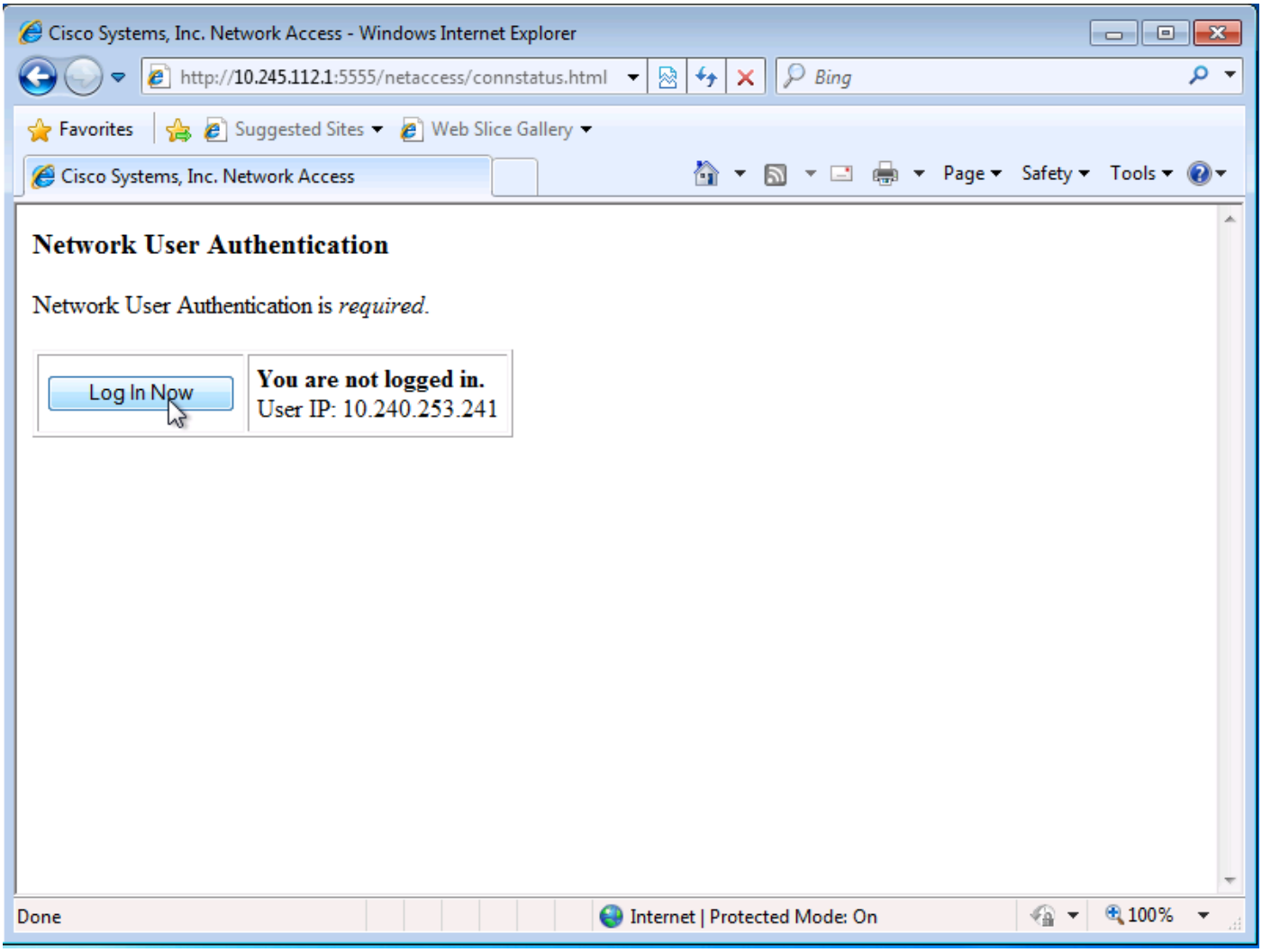
```
ciscoasa(config)# show asp table socket

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

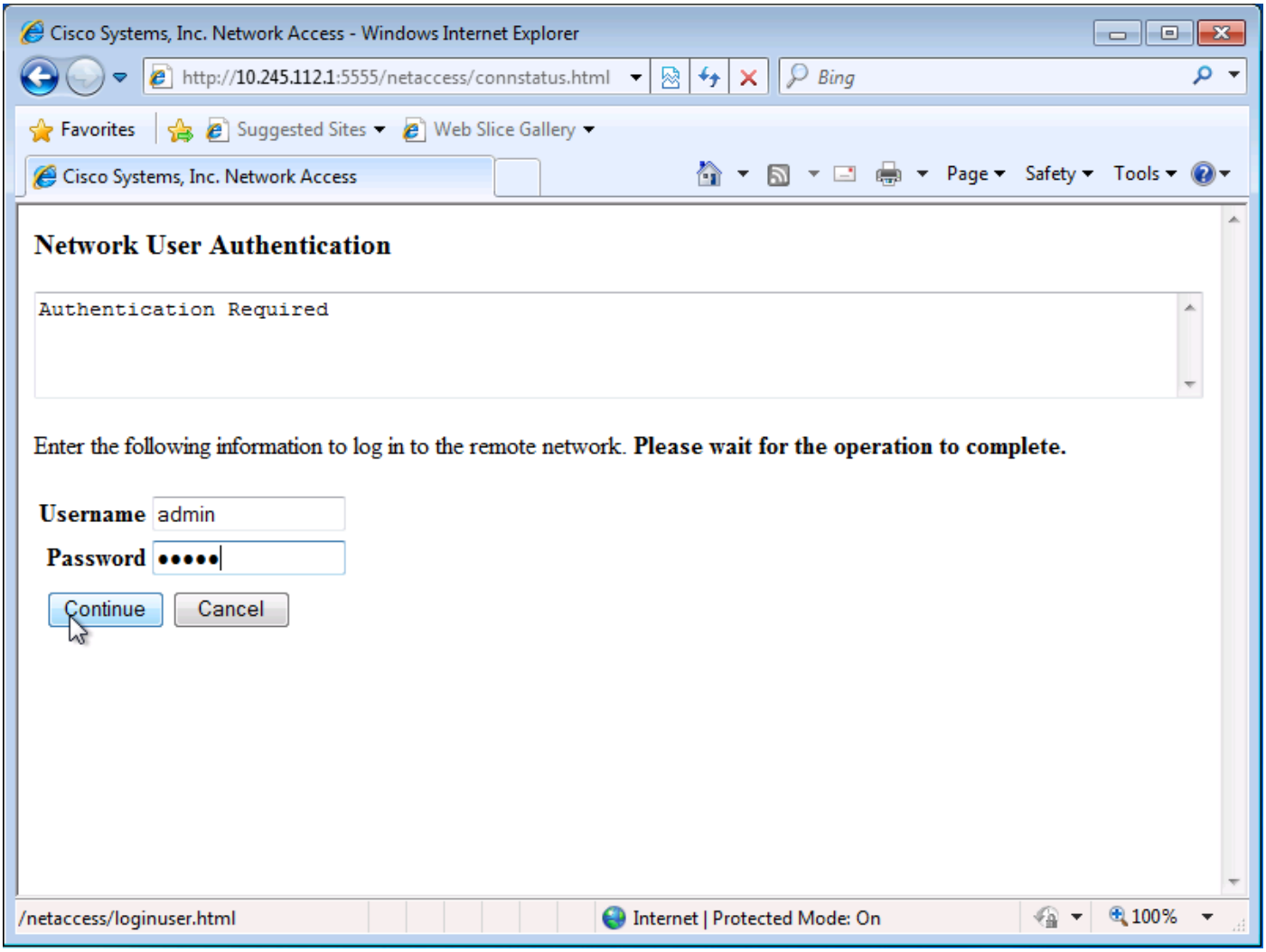
Después de configurar el ASA como se muestra arriba, un intento de conexión a través del ASA a un host externo en el puerto TCP 3389 dará lugar a una denegación de conexión. El usuario primero debe autenticarse para permitir el tráfico TCP/3389.

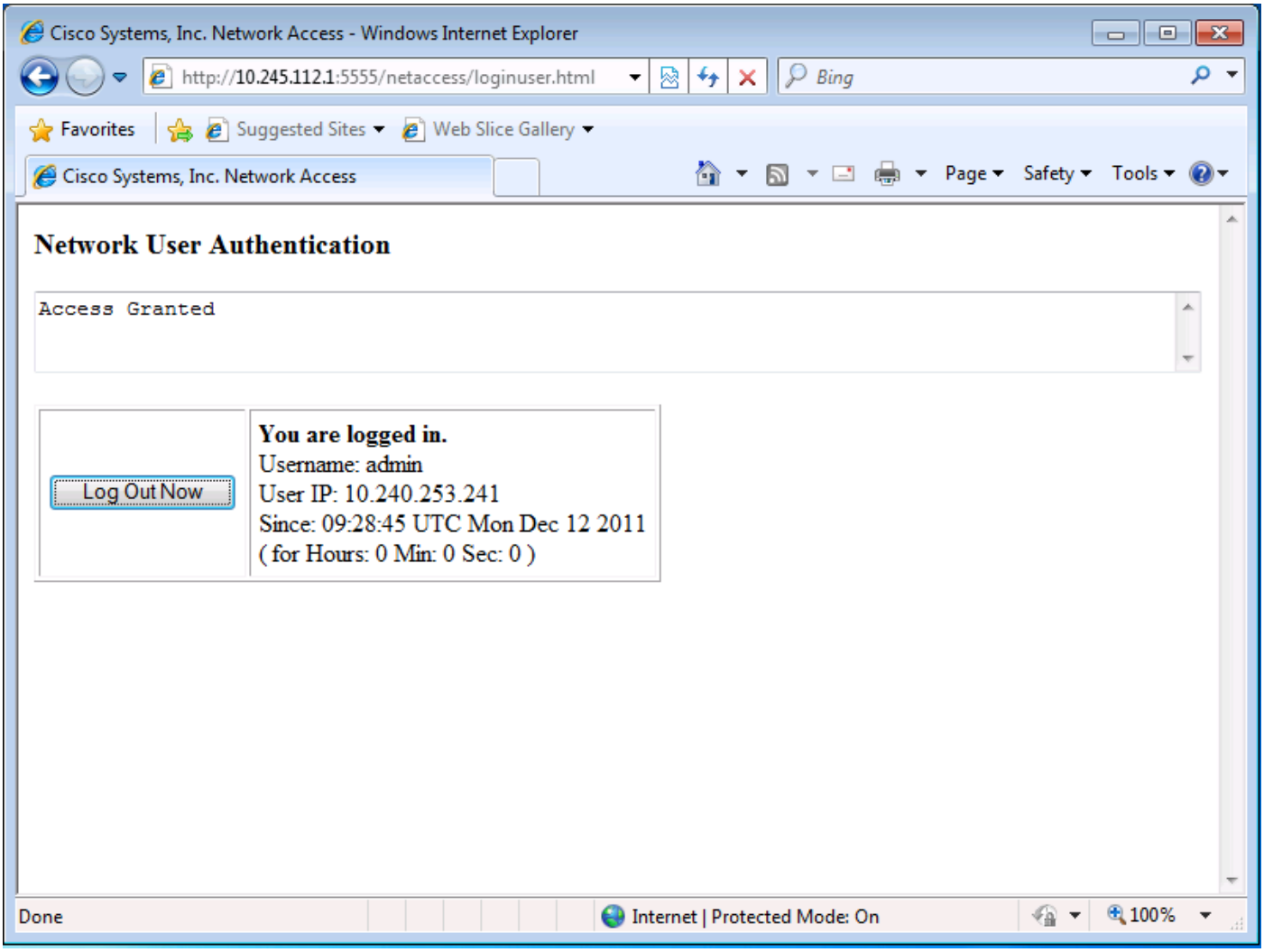
La autenticación directa requiere que el usuario busque directamente el ASA. Si navega a http://<*asa_ip*>:<*port*>, se devuelve un error 404 porque no existe ninguna página web en la raíz del servidor web del ASA.



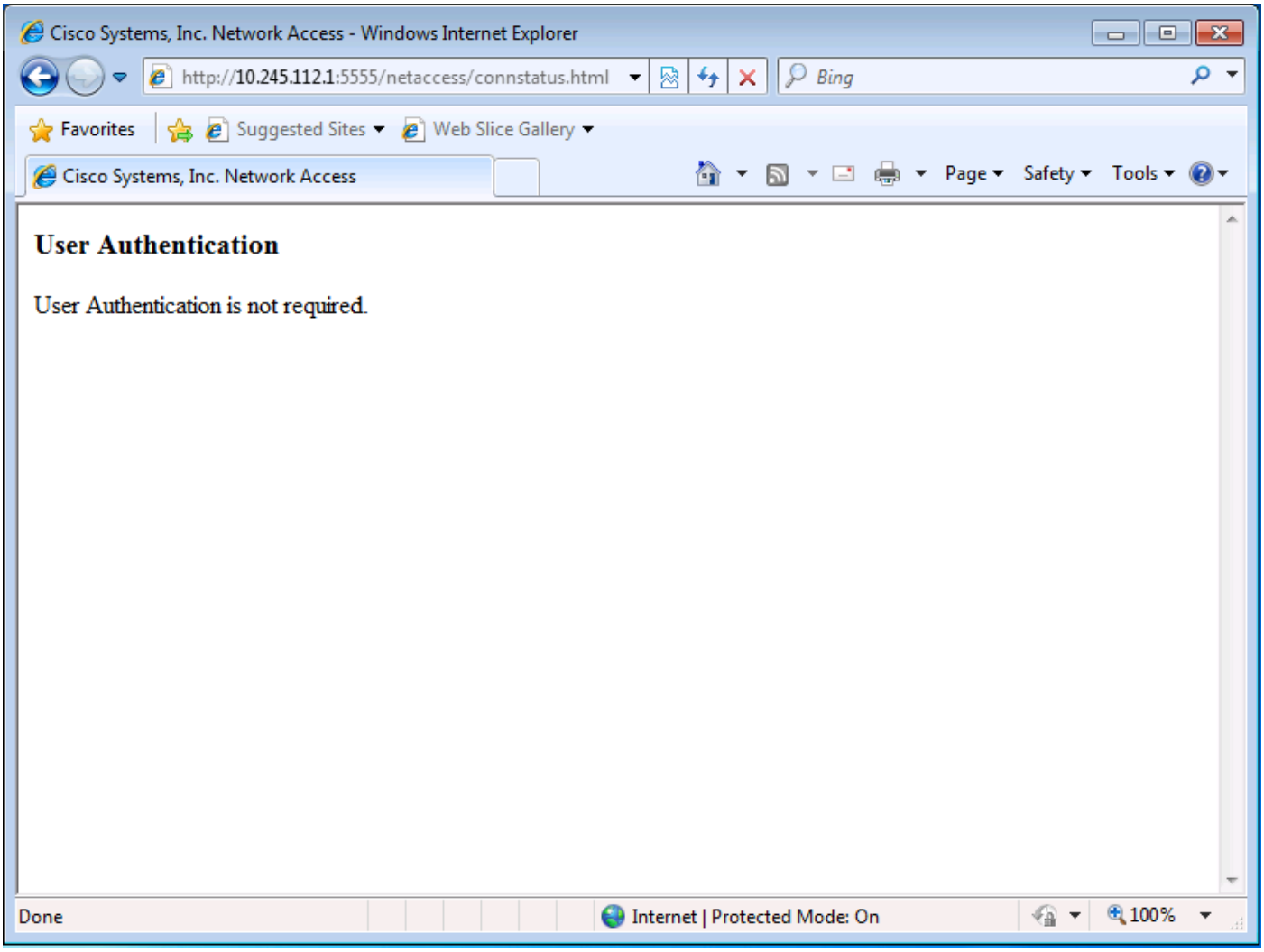
En su lugar, debe navegar directamente a http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html. Una página de inicio de sesión se encuentra en esta URL, donde puede proporcionar credenciales de autenticación.


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%



En esta configuración, el tráfico de autenticación directa forma parte de la lista de acceso authmatch. Sin esta entrada de control de acceso, es posible que reciba un mensaje inesperado, como *Autenticación de usuario, no se requiere autenticación de usuario,* cuando navega a http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html.



Después de autenticarse correctamente, puede conectarse a través del ASA a un servidor externo en TCP/3389.