# Exemplo de configuração de autenticação direta e cut-through ASA

## Contents



## Introduction

Este documento descreve como configurar a autenticação rápida e direta no ASA.

## Prerequisites

### Requirements

Não existem requisitos específicos para este documento.

### Componentes Utilizados

As informações neste documento são baseadas no Cisco Adaptive Security Appliance (ASA).

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico.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.

### Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

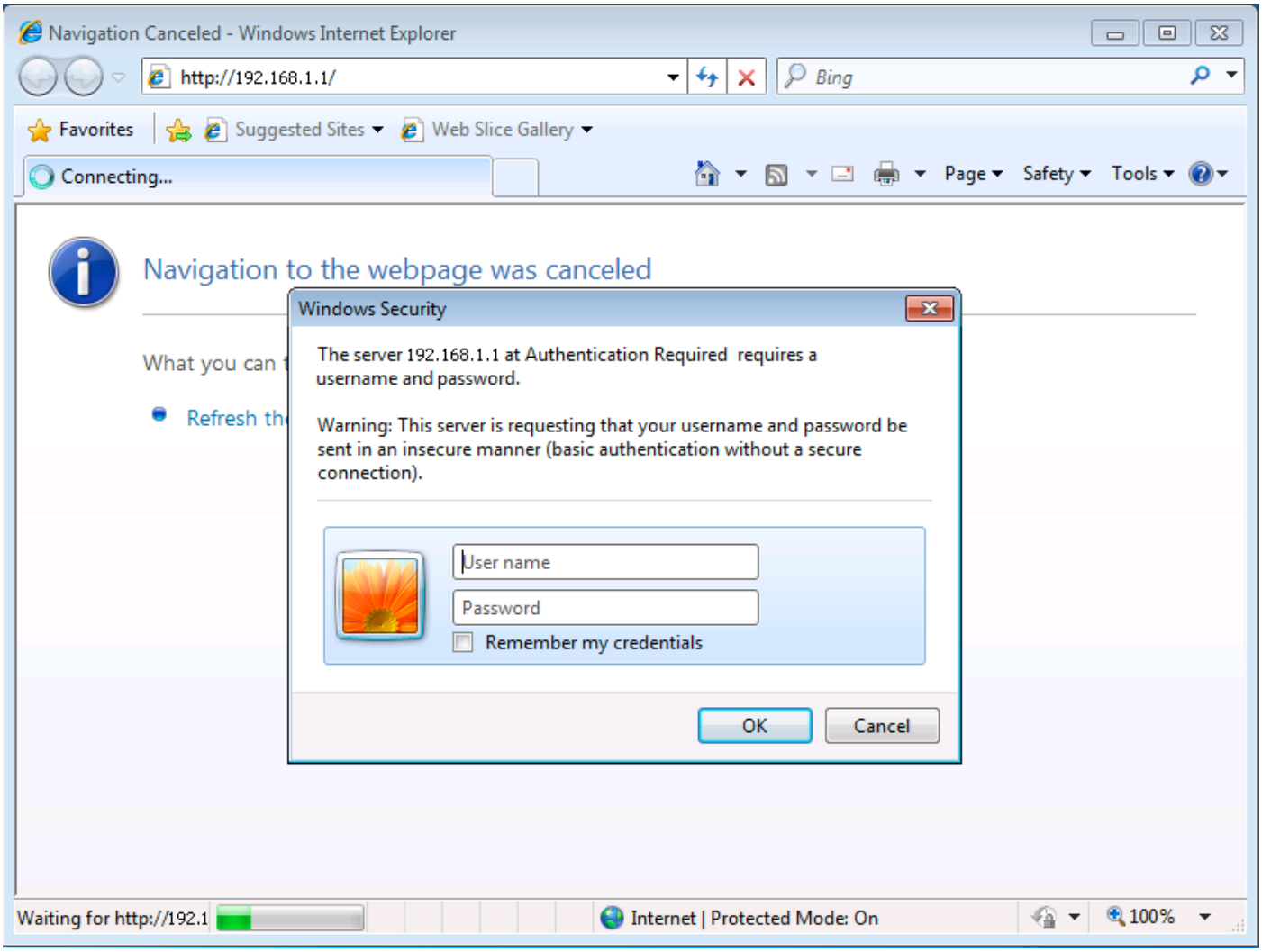
## Cut-Through

A autenticação cut-through foi configurada anteriormente com o comando **aaa authentication include**. Agora, o comando **aaa authentication match** é usado. O tráfego que requer autenticação é permitido em uma lista de acesso referenciada pelo comando **aaa authentication match**, que faz com que o host seja autenticado antes que o tráfego especificado seja permitido através do ASA.

Aqui está um exemplo de configuração para autenticação de tráfego da Web:

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

Observe que essa solução funciona porque o HTTP é um protocolo no qual o ASA pode injetar autenticação. O ASA intercepta o tráfego HTTP e o autentica via autenticação HTTP. Como a autenticação é injetada em linha, uma caixa de diálogo de autenticação HTTP aparece no navegador da Web como mostrado nesta imagem:




# Autenticação direta

A autenticação direta foi previamente configurada com os comandos **aaa authentication include** e **virtual < protocol>**. Agora, os comandos **aaa authentication match** e **aaa authentication listener** são usados.

Para protocolos que não suportam autenticação nativa (ou seja, protocolos que não podem ter um desafio de autenticação em linha), a autenticação ASA direta pode ser configurada. Por padrão, o ASA não ouve solicitações de autenticação. Um ouvinte pode ser configurado em uma porta e interface específica com o comando **aaa authentication listener**.

Este é um exemplo de configuração que permite o tráfego TCP/3389 através do ASA depois que um host é autenticado:

```
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
```

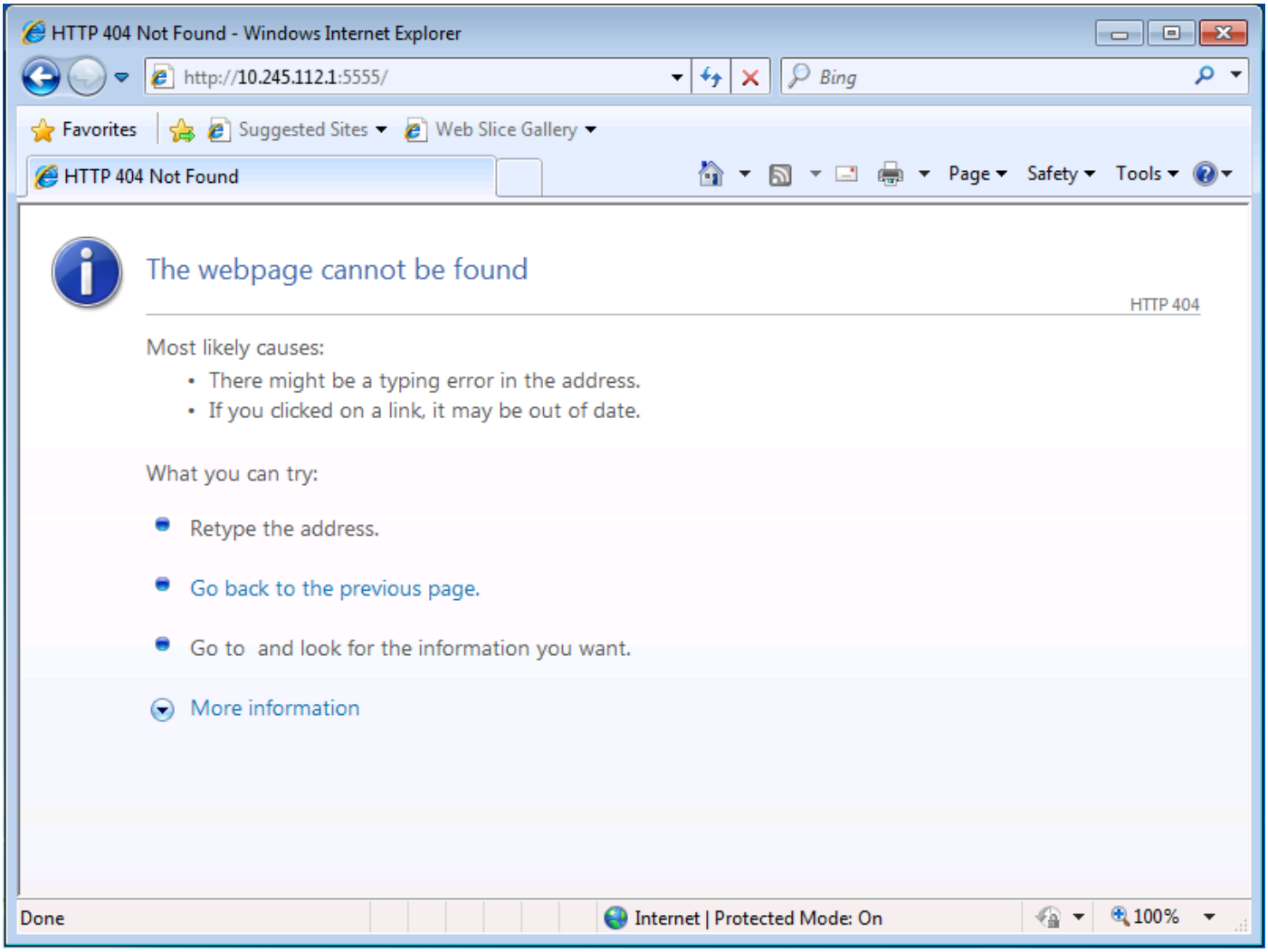
Observe o número de porta usado pelo ouvinte (TCP/5555). A saída do comando **show asp table socket** mostra que o ASA agora escuta solicitações de conexão a esta porta no endereço IP atribuído à interface (interna) especificada.

```
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)#
```

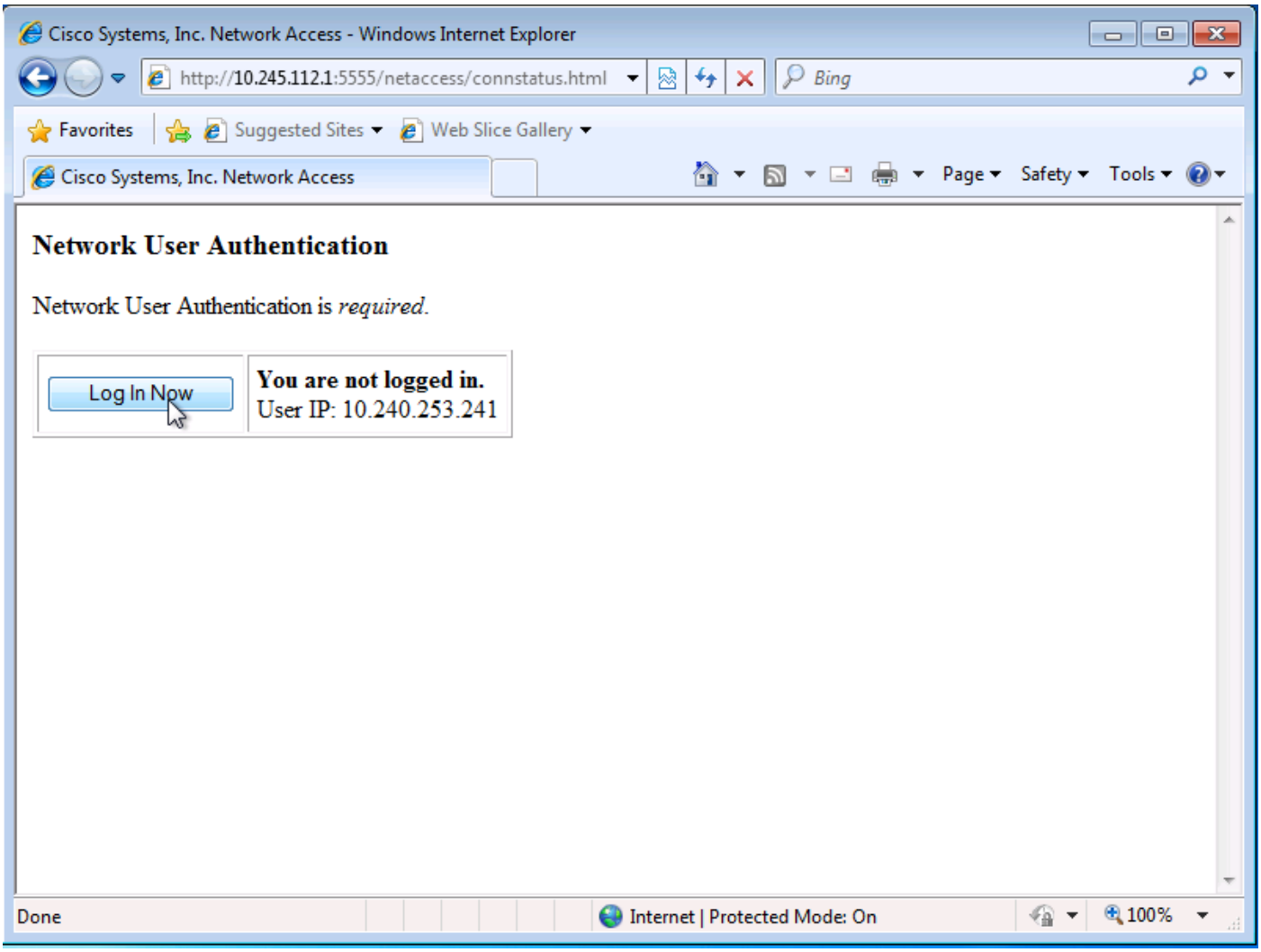
Depois que o ASA é configurado conforme mostrado acima, uma tentativa de conexão através do ASA com um host externo na porta TCP 3389 resultará em uma negação de conexão. O usuário deve primeiro autenticar o tráfego TCP/3389 para ser permitido.

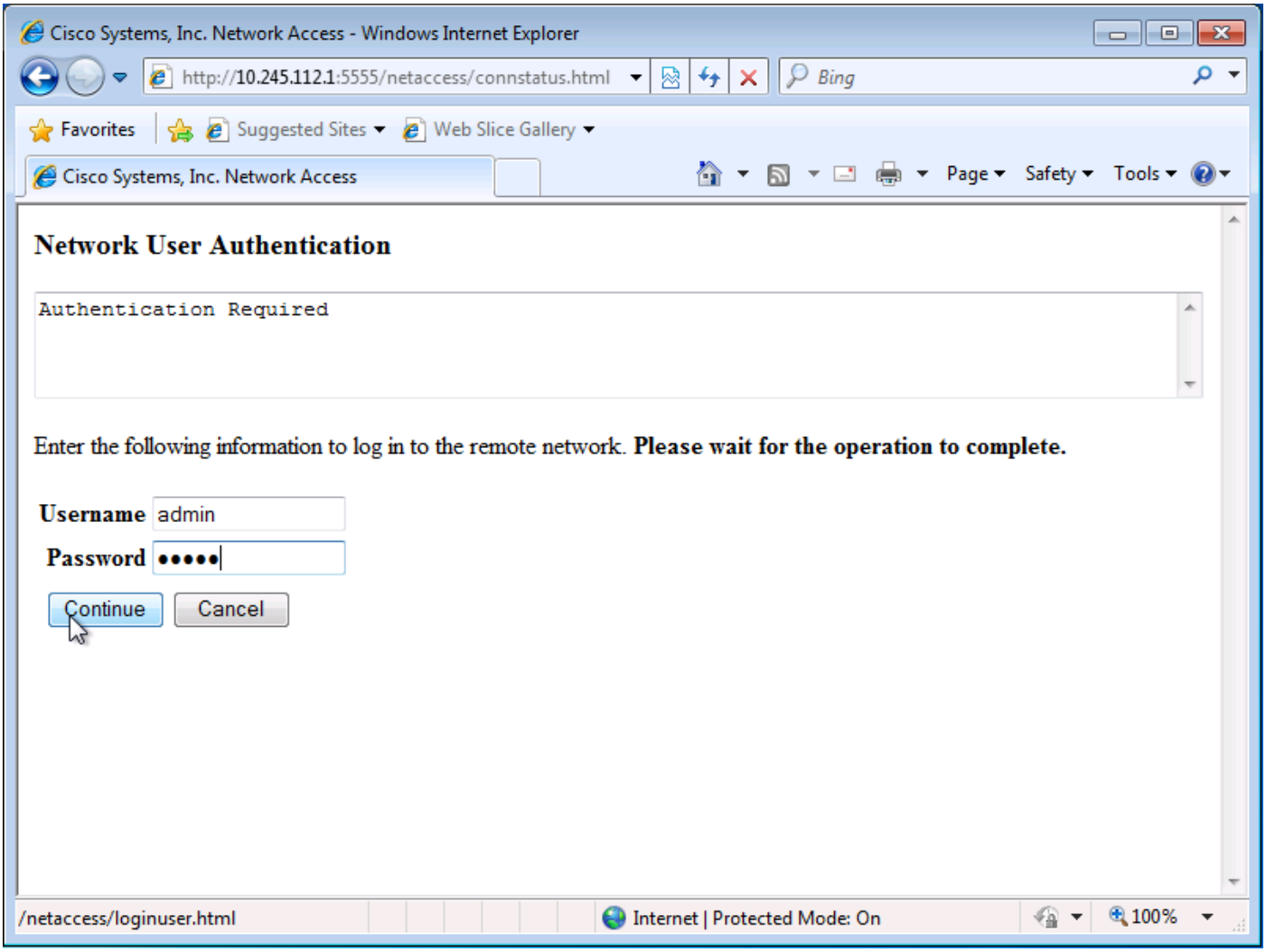
A autenticação direta exige que o usuário navegue diretamente para o ASA. Se você navegar até http://<*asa_ip*>:<*port*>, um erro 404 será retornado porque não há nenhuma página da Web na raiz do servidor da Web do ASA.

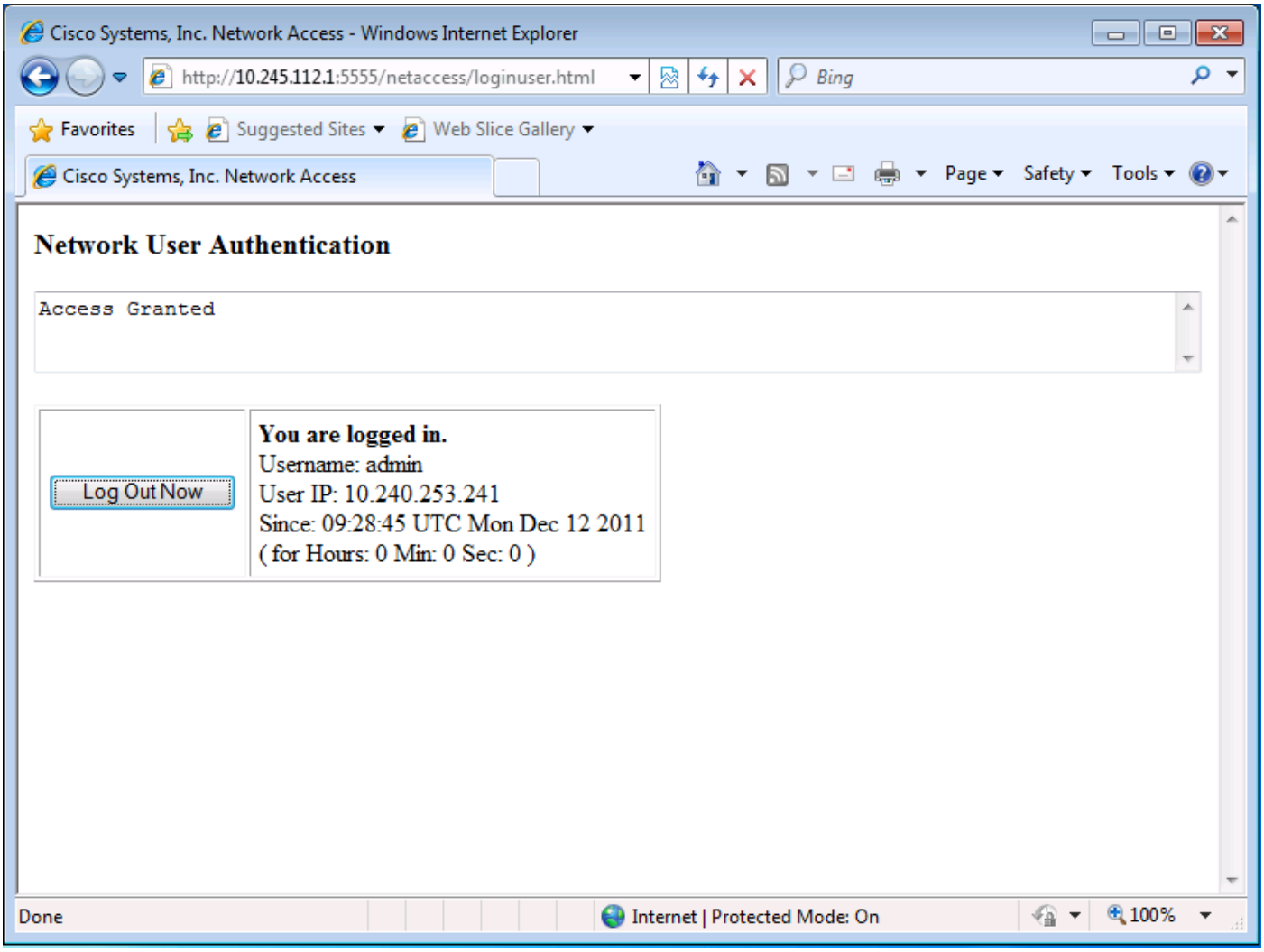



Em vez disso, você deve navegar diretamente para

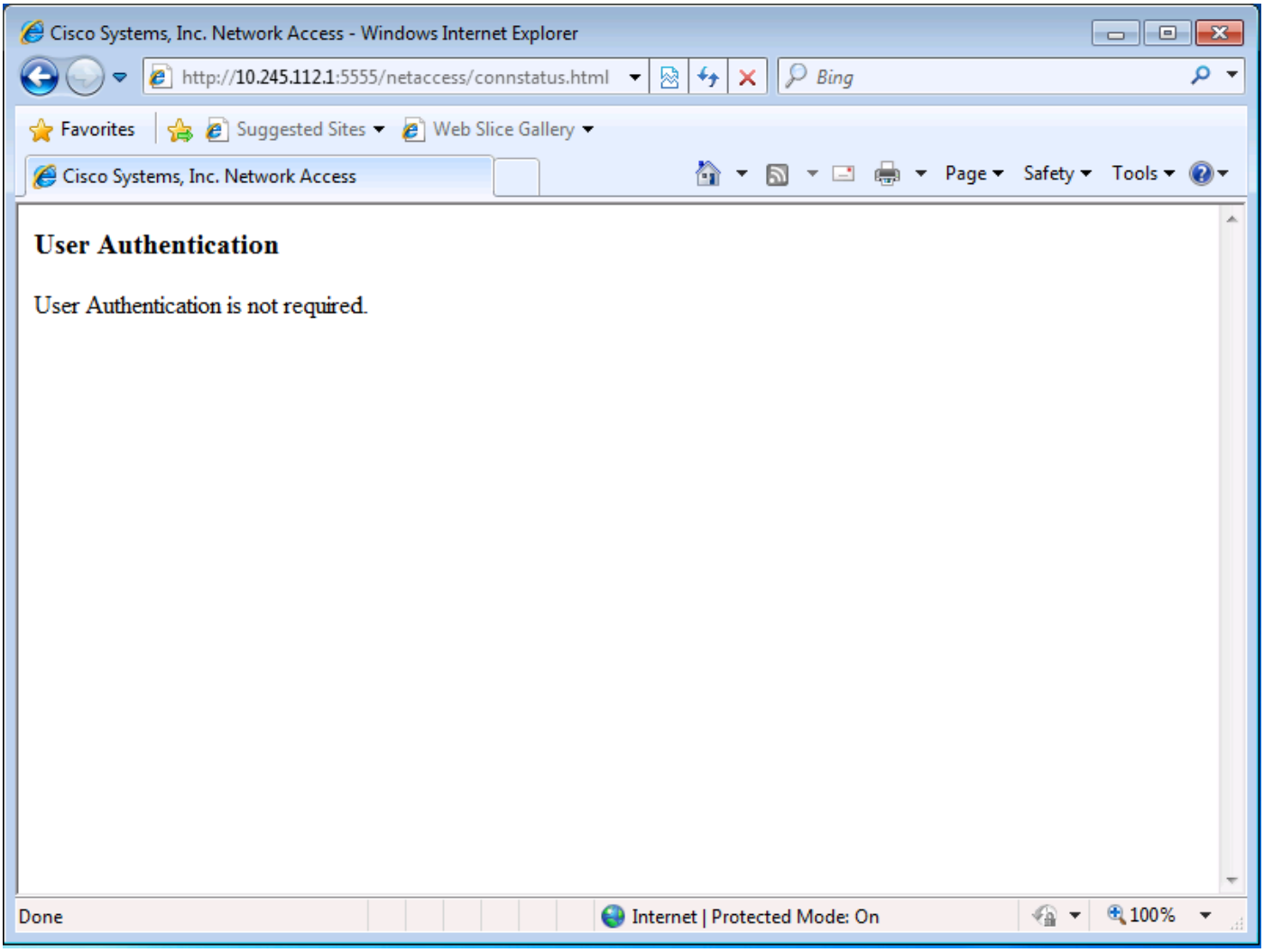
http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html. Uma página de login reside neste URL onde você pode fornecer credenciais de autenticação.




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%




Nesta configuração, o tráfego de autenticação direta faz parte da lista de acesso de correspondência de autenticação. Sem esta entrada de controle de acesso, você pode receber uma mensagem inesperada, como *User Authentication, User Authentication is not required,* quando navegar até http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html.




Depois de autenticar com êxito, você pode se conectar através do ASA a um servidor externo no TCP/3389.