Exemple de configuration de l'authentification ASA directe et cut-through

Contenu

Introduction

Ce document décrit comment configurer l'authentification ASA directe et directe.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations de ce document sont basées sur l'appliance de sécurité adaptative (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.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco.](#)

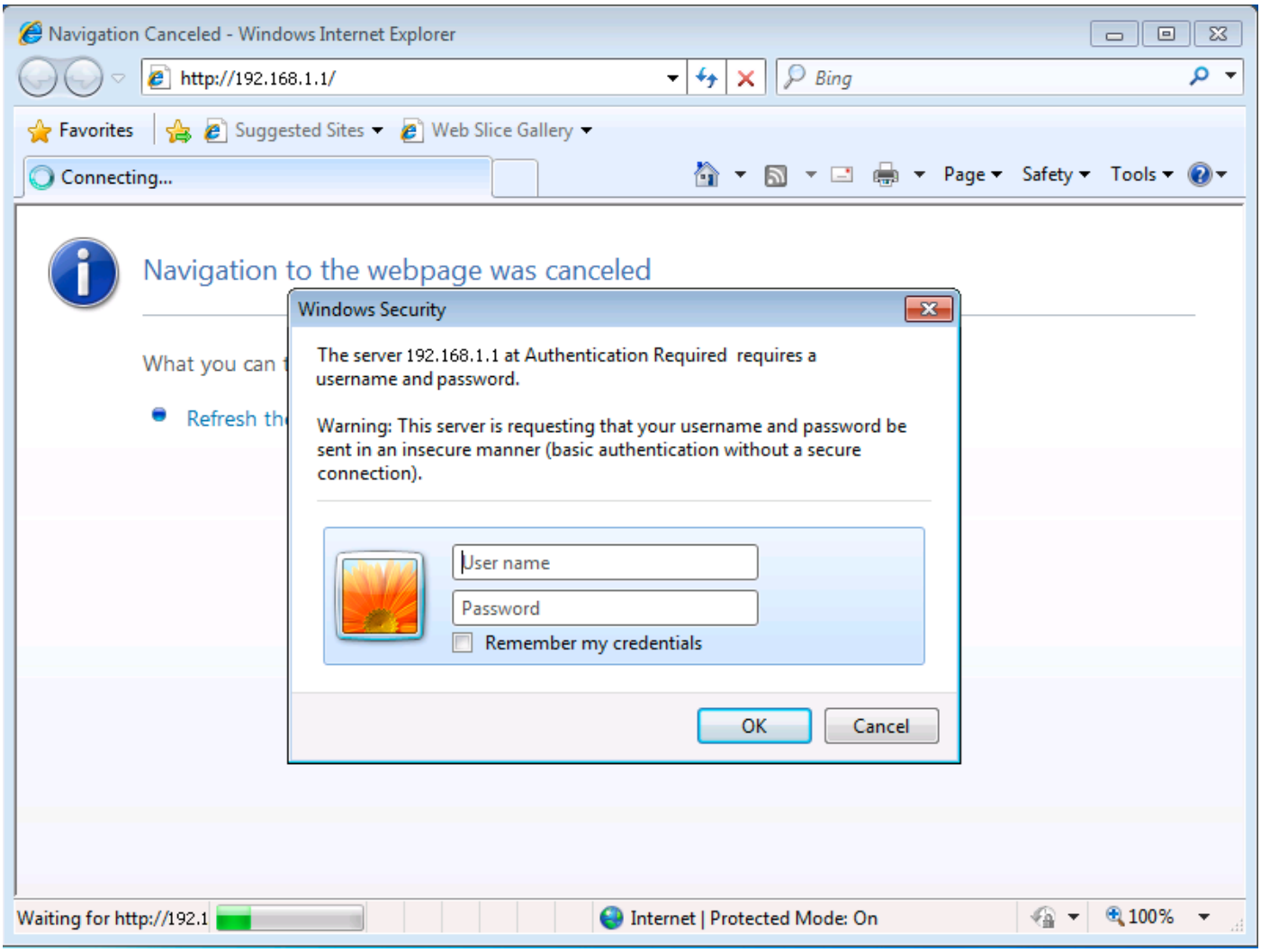
Cut-through

L'authentification cut-through a été précédemment configurée avec la commande **aaa authentication include**. Maintenant, la commande **aaa authentication match** est utilisée. Le trafic qui nécessite une authentification est autorisé dans une liste d'accès référencée par la commande **aaa authentication match**, ce qui entraîne l'authentification de l'hôte avant que le trafic spécifié ne soit autorisé par l'ASA.

Voici un exemple de configuration pour l'authentification du trafic Web :

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

Notez que cette solution fonctionne car HTTP est un protocole dans lequel l'ASA peut injecter l'authentification. L'ASA intercepte le trafic HTTP et l'authentifie via l'authentification HTTP. Étant donné que l'authentification est injectée en ligne, une boîte de dialogue d'authentification HTTP apparaît dans le navigateur Web, comme illustré dans cette image :



Authentification directe

L'authentification directe a été précédemment configurée avec les commandes **aaa authentication include** et **virtual < protocol>**. Maintenant, les commandes **aaa authentication match** et **aaa authentication listener** sont utilisées.

Pour les protocoles qui ne prennent pas en charge l'authentification nativement (c'est-à-dire les protocoles qui ne peuvent pas avoir de défi d'authentification en ligne), l'authentification ASA directe peut être configurée. Par défaut, l'ASA n'écoute pas les demandes d'authentification. Un écouteur peut être configuré sur un port et une interface particuliers à l'aide de la commande **aaa authentication listener**.

Voici un exemple de configuration qui autorise le trafic TCP/3389 via l'ASA une fois qu'un hôte a

été authentifié :

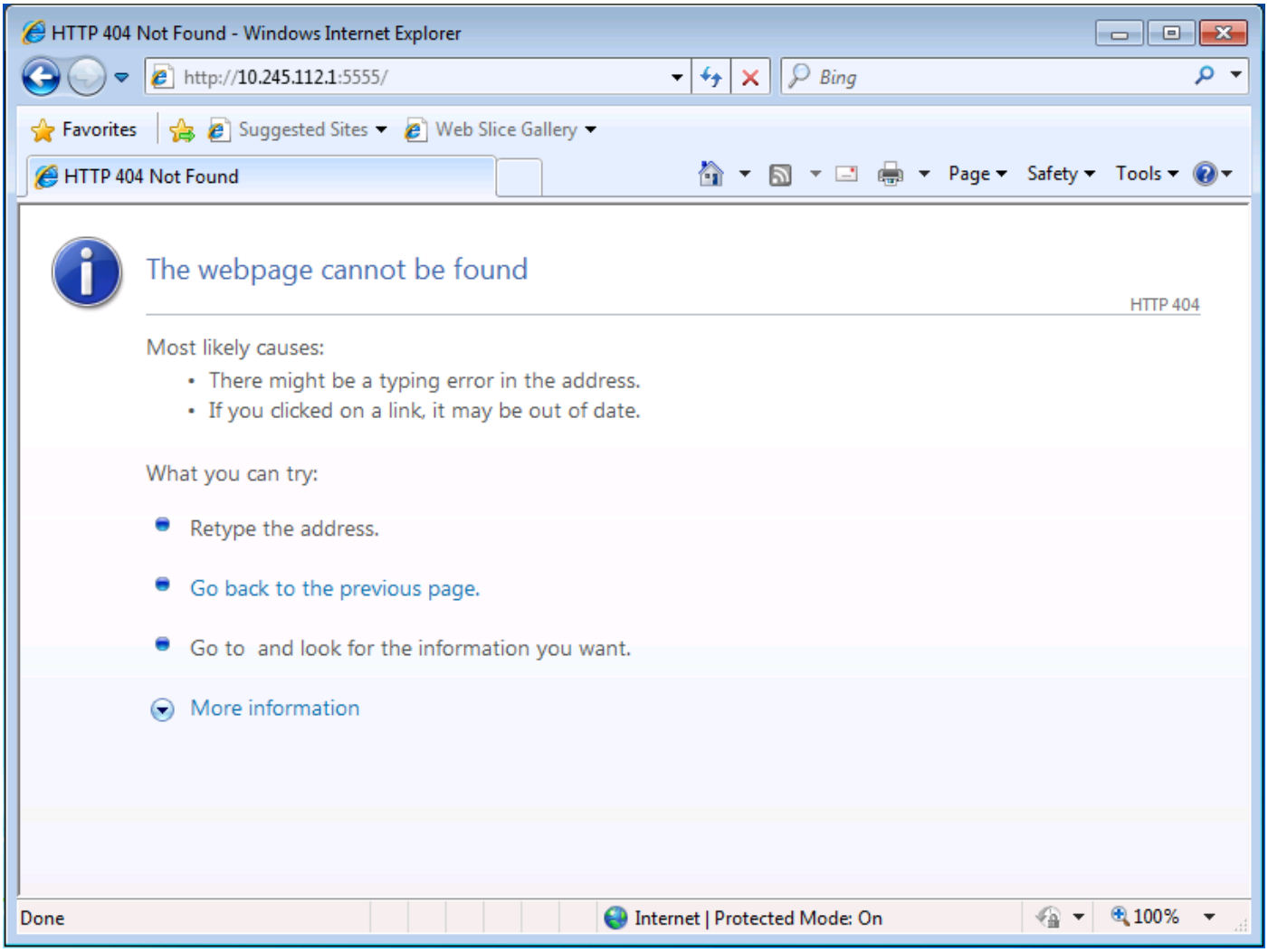
```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 3389
access-list authmatch permit tcp any host 10.245.112.1 eq 5555
aaa authentication match authmatch inside LOCAL
aaa authentication listener http inside port 5555
```

Notez le numéro de port utilisé par l'écouteur (TCP/5555). La sortie de la commande **show asp table socket** montre que l'ASA écoute maintenant les demandes de connexion à ce port à l'adresse IP attribuée à l'interface (interne) spécifiée.

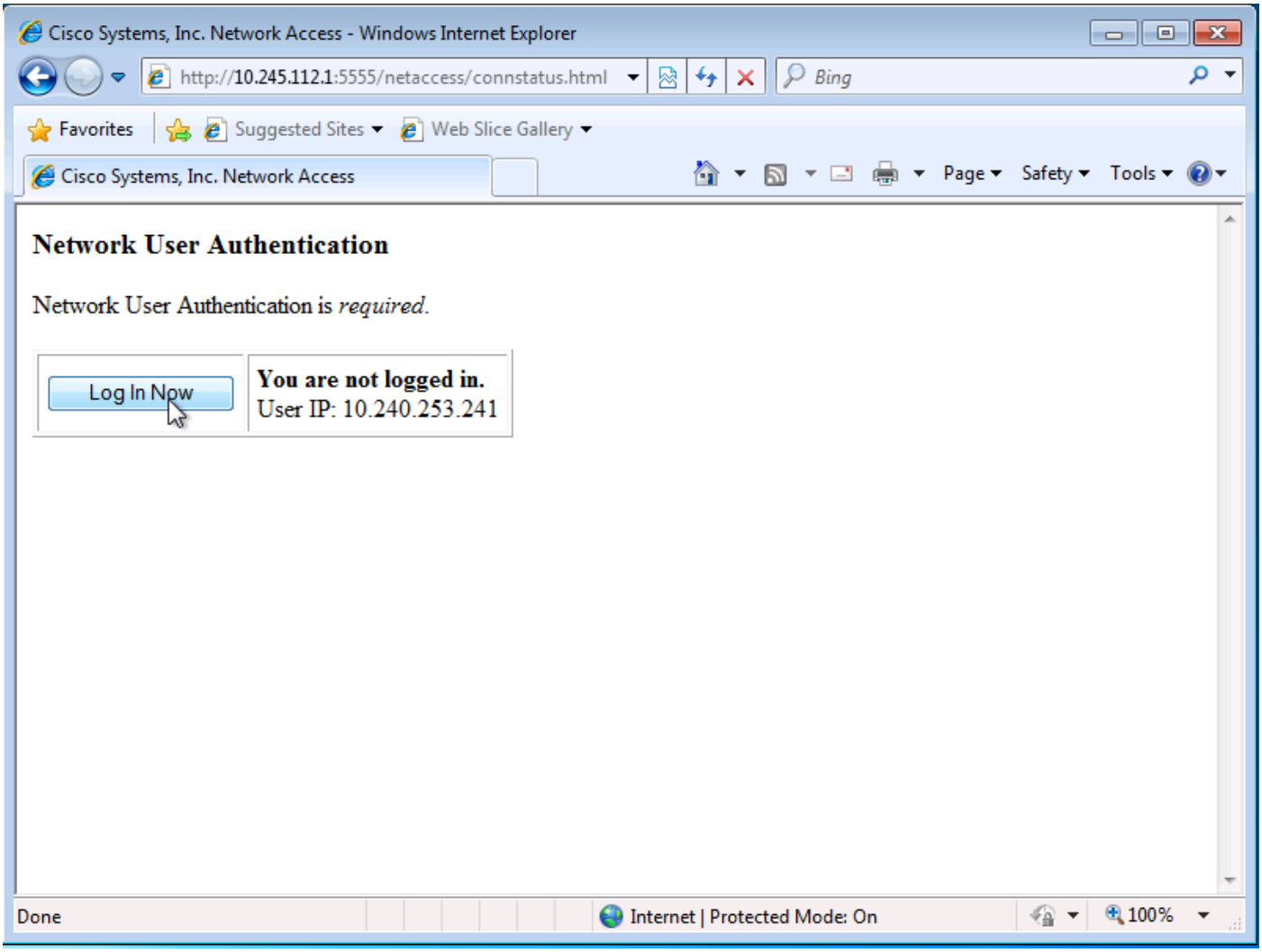
```
ciscoasa(config)# show asp table socket

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

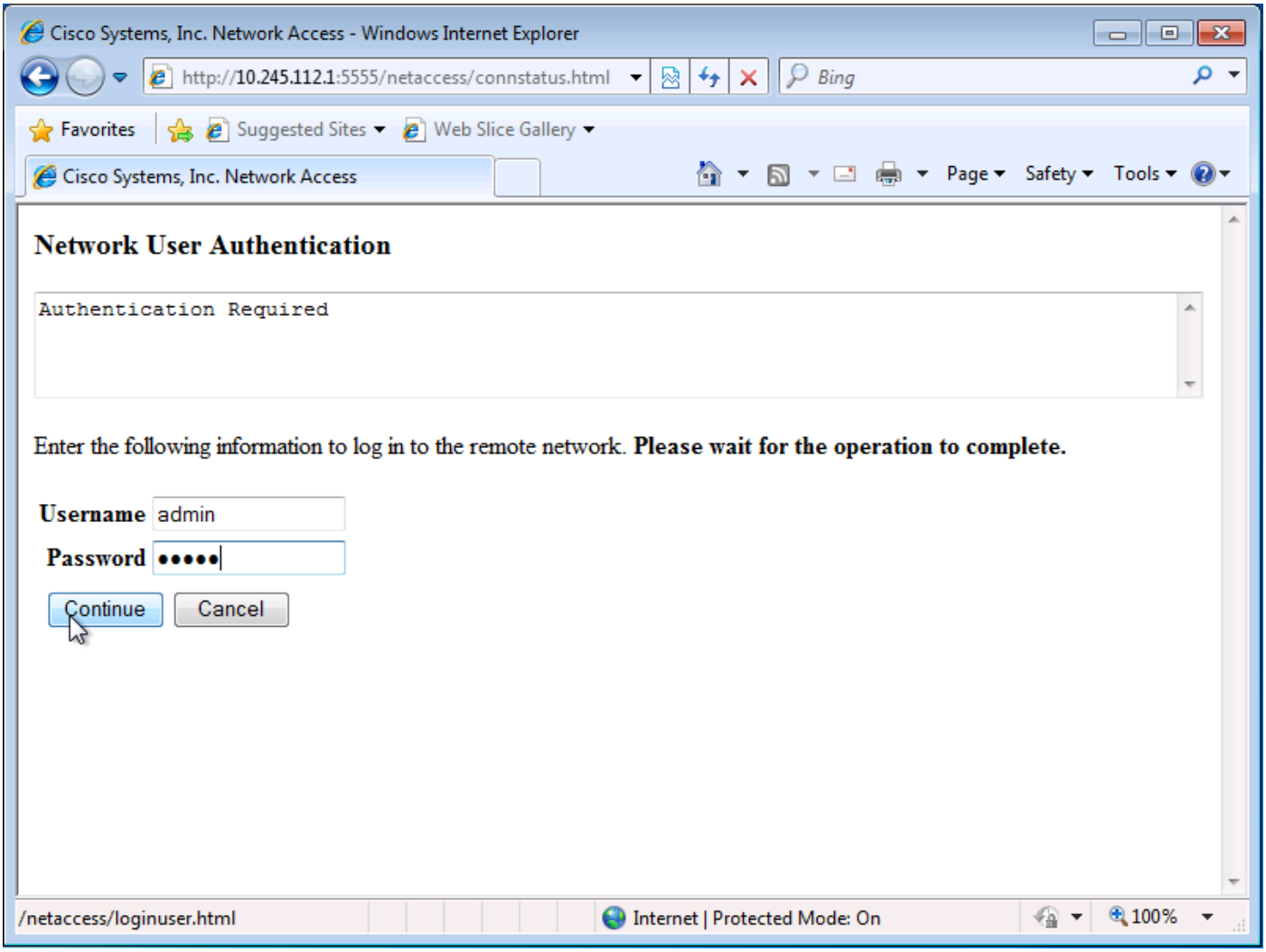
Une fois l'ASA configuré comme indiqué ci-dessus, une tentative de connexion via l'ASA à un hôte externe sur le port TCP 3389 entraînera un déni de connexion. L'utilisateur doit d'abord s'authentifier pour autoriser le trafic TCP/3389.

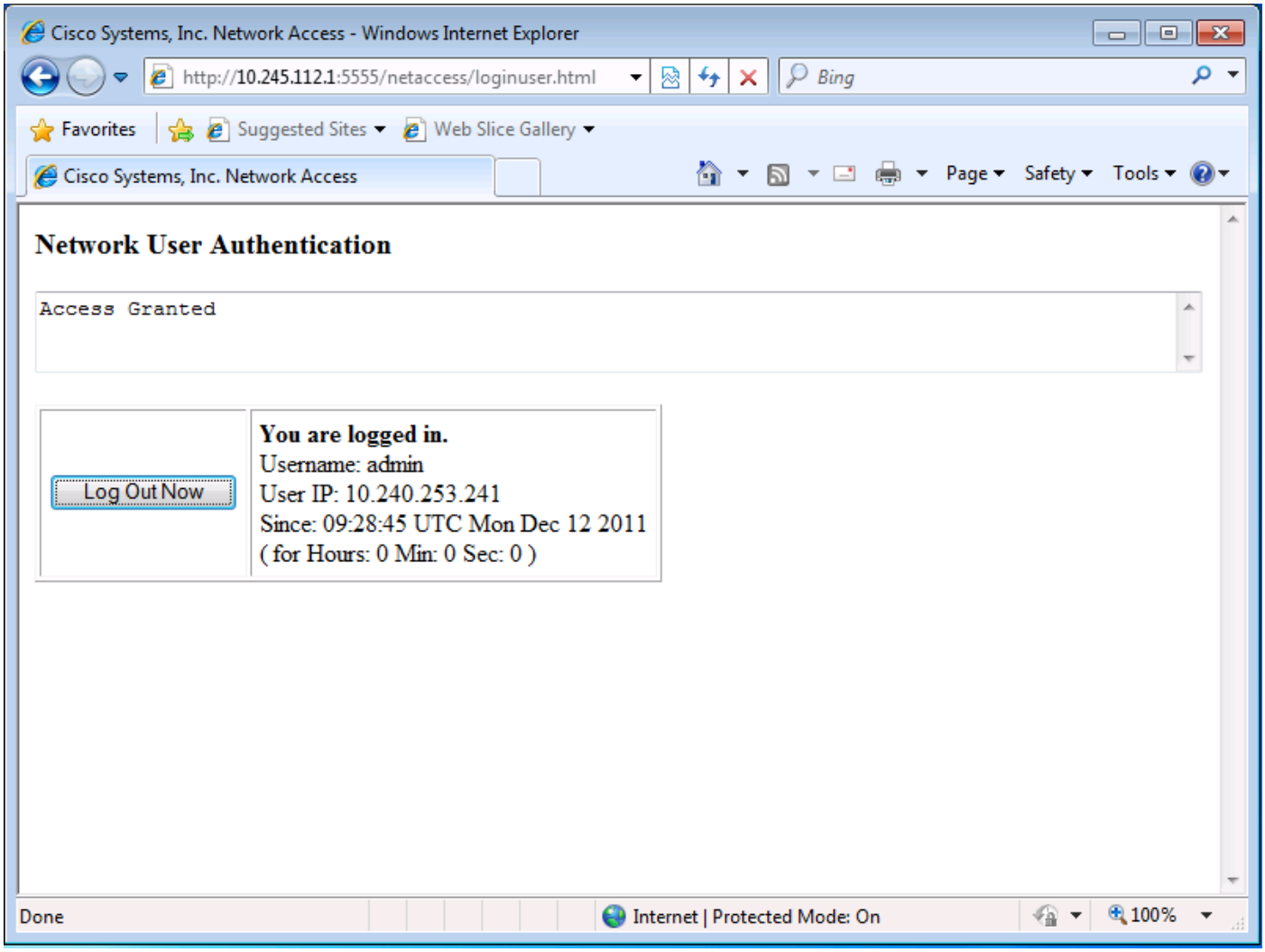
L'authentification directe nécessite que l'utilisateur accède directement à l'ASA. Si vous accédez à http://<*asa_ip*>:<*port*>, une erreur 404 est renvoyée car aucune page Web n'existe à la racine du serveur Web ASA.



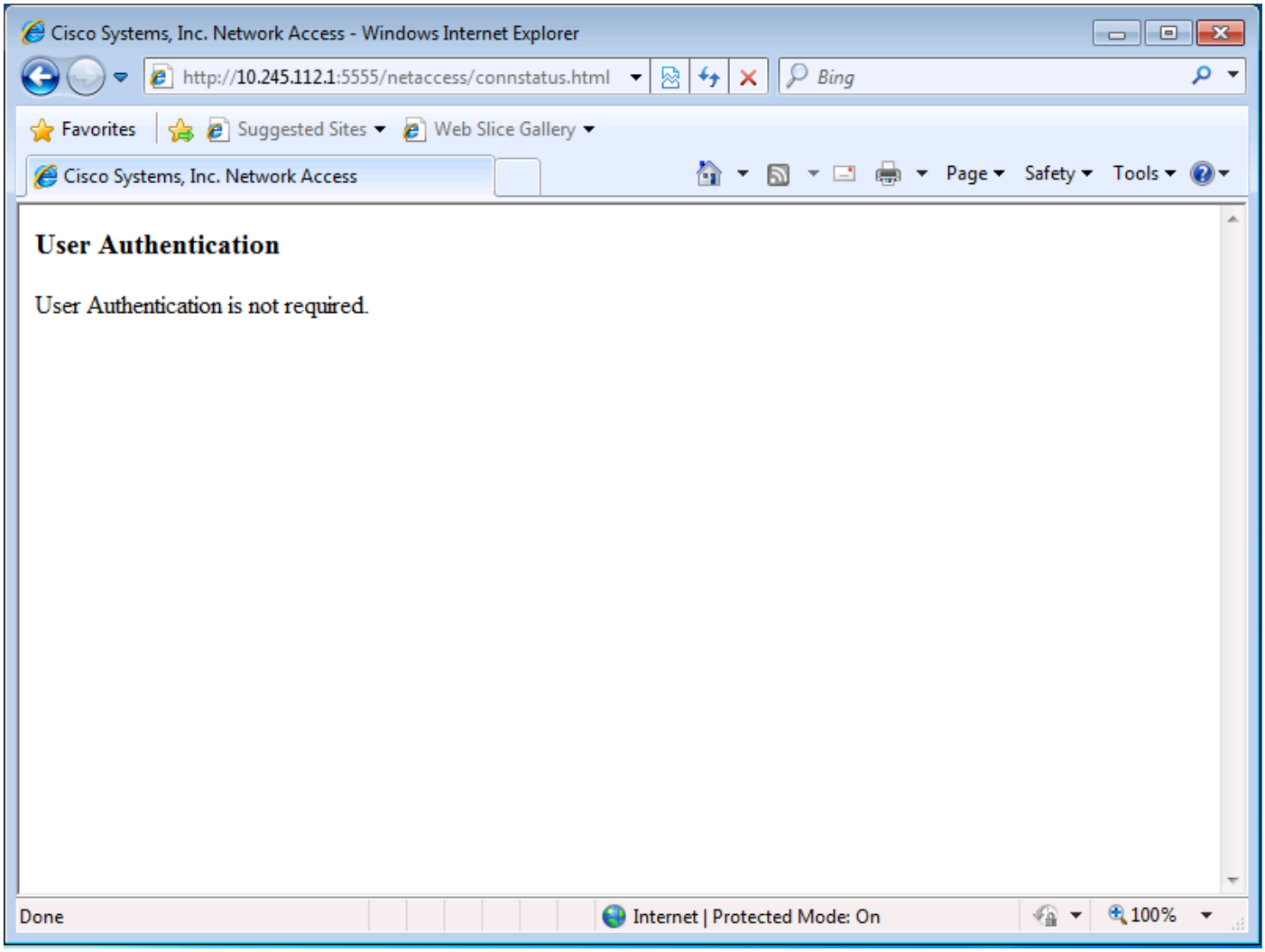
Vous devez plutôt naviguer directement sur http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html. Une page de connexion se trouve à cette URL où vous pouvez fournir des informations d'identification d'authentification.


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%



Dans cette configuration, le trafic d'authentification directe fait partie de la liste d'accès authmatch. Sans cette entrée de contrôle d'accès, vous pouvez recevoir un message inattendu, tel que *Authentification utilisateur, Authentification utilisateur non requise,* lorsque vous accédez à http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html.



Une fois l'authentification terminée, vous pouvez vous connecter à un serveur externe via l'ASA sur TCP/3389.