Configuratievoorbeeld van Cut-Through en Direct ASA-verificatie

Inhoud

Inleiding

Dit document beschrijft hoe u de doorlopende en directe ASA-verificatie kunt configureren.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco adaptieve security applicatie (ASA).

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg [Cisco Technical Tips Conventions (Conventies voor technische tips van Cisco) voor meer informatie over documentconventies.](#)

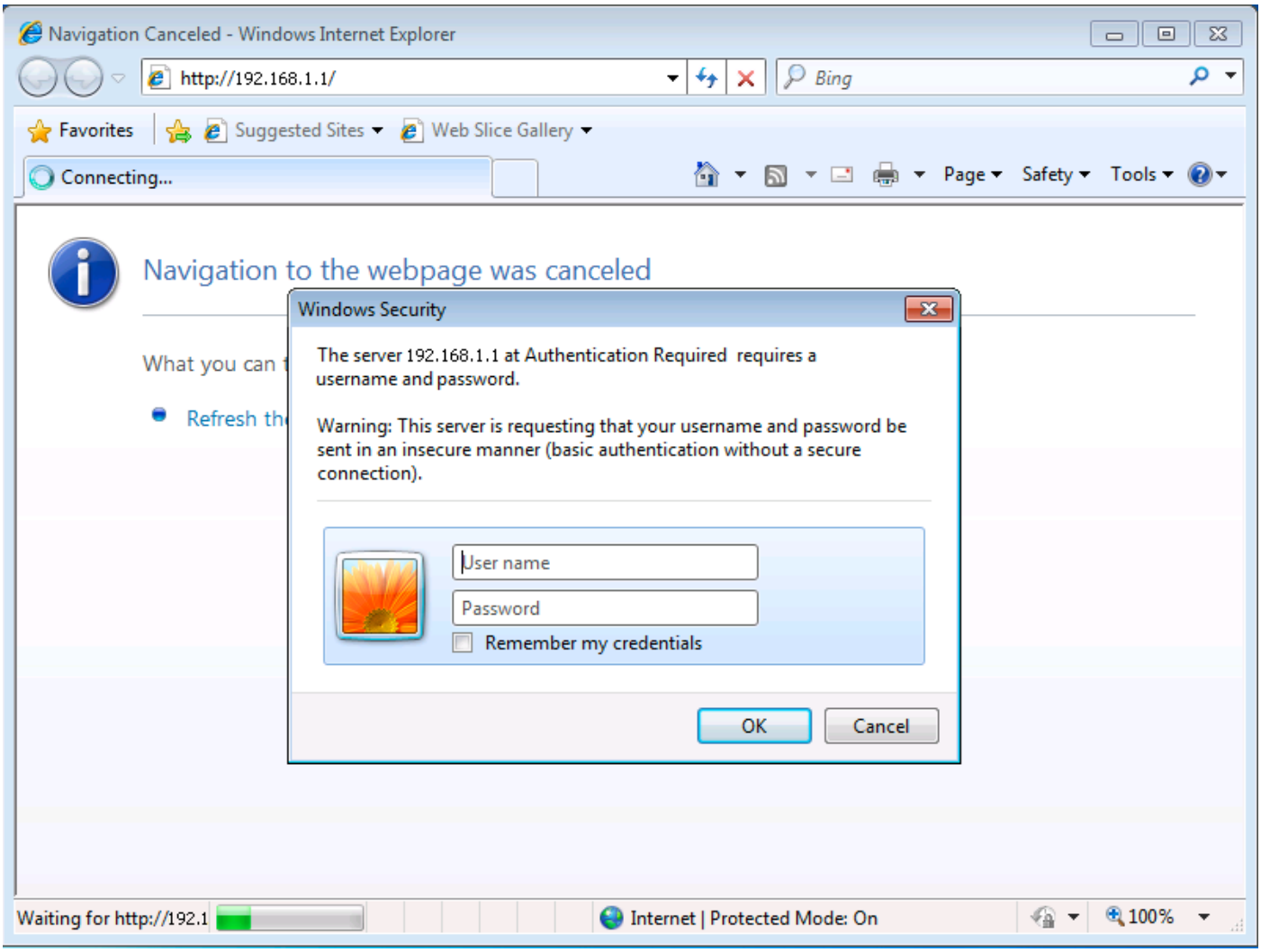
doorsnede

Snijd-door-verificatie werd eerder ingesteld met **onder meer** opdracht **voor** verificatie. Nu wordt de opdracht **van de** verificatiematch gebruikt. Verkeersverkeer dat verificatie vereist is toegestaan in een toegangslijst die van referentie is door de opdracht **van de** echtheidscontrole, die ervoor zorgt dat de host geauthentificeerd wordt voordat het gespecificeerde verkeer door de ASA is toegestaan.

Hier is een configuratievoorbeeld voor web traffic authenticatie:

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

Merk op dat deze oplossing werkt omdat HTTP een protocol is waarin de ASA verificatie kan injecteren. ASA onderschept HTTP-verkeer en authenticeert het via HTTP-verificatie. Omdat de authenticatie inline geïnjecteerd wordt, verschijnt een HTTP authenticatie dialoogvenster in de webbrowser zoals in deze afbeelding getoond wordt:



Direct-verificatie

Direct authenticatie werd eerder ingesteld met de **aaa authenticatie** en **virtuele < protocol>** opdrachten. Nu, de **aaa authenticatie match** en **de** opdrachten van de **authenticatie** worden gebruikt.

Voor protocollen die geen authenticatie ondersteunen (dat wil zeggen, protocollen die niet online een authenticatie-uitdaging kunnen hebben), kan de directe ASA-verificatie worden geconfigureerd. Standaard luistert de ASA niet naar verificatieverzoeken. Een luisteraar kan op een bepaalde poort en interface met de opdracht **van de** verificatieluisteraar worden ingesteld.

Hier is een configuratievoorbeeld dat TCP/3389-verkeer door de ASA toestaat zodra een host is geauthentiseerd:

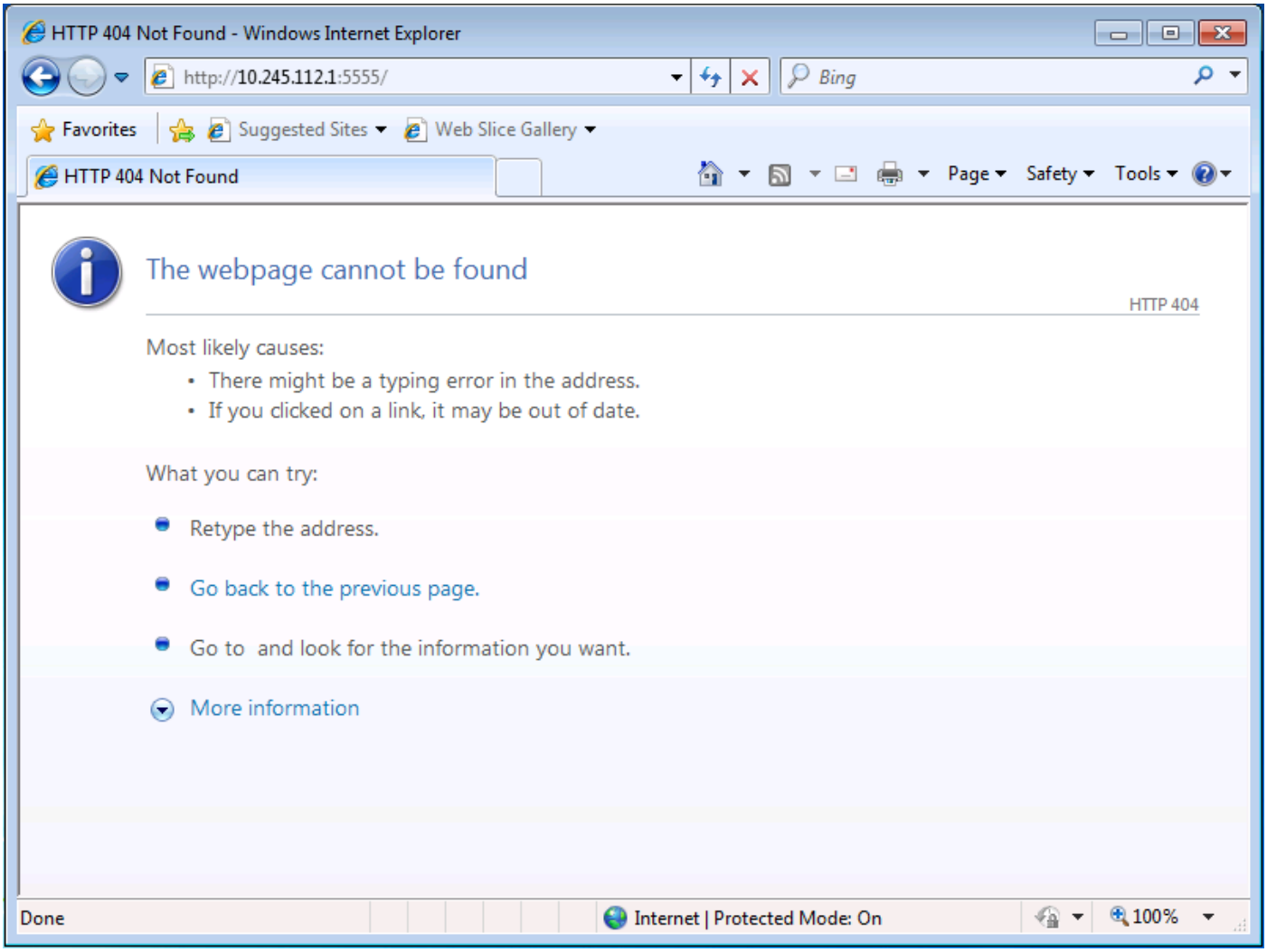
```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 3389
access-list authmatch permit tcp any host 10.245.112.1 eq 5555
aaa authentication match authmatch inside LOCAL
aaa authentication listener http inside port 5555
```

Let op het poortnummer dat door de luisteraar wordt gebruikt (TCP/5555). De opdrachtoutput **van het** asp-stopcontact toont dat de ASA nu naar aansluitingsverzoeken op deze poort luistert op het IP-adres dat is toegewezen aan de gespecificeerde (binnenkant) interface.

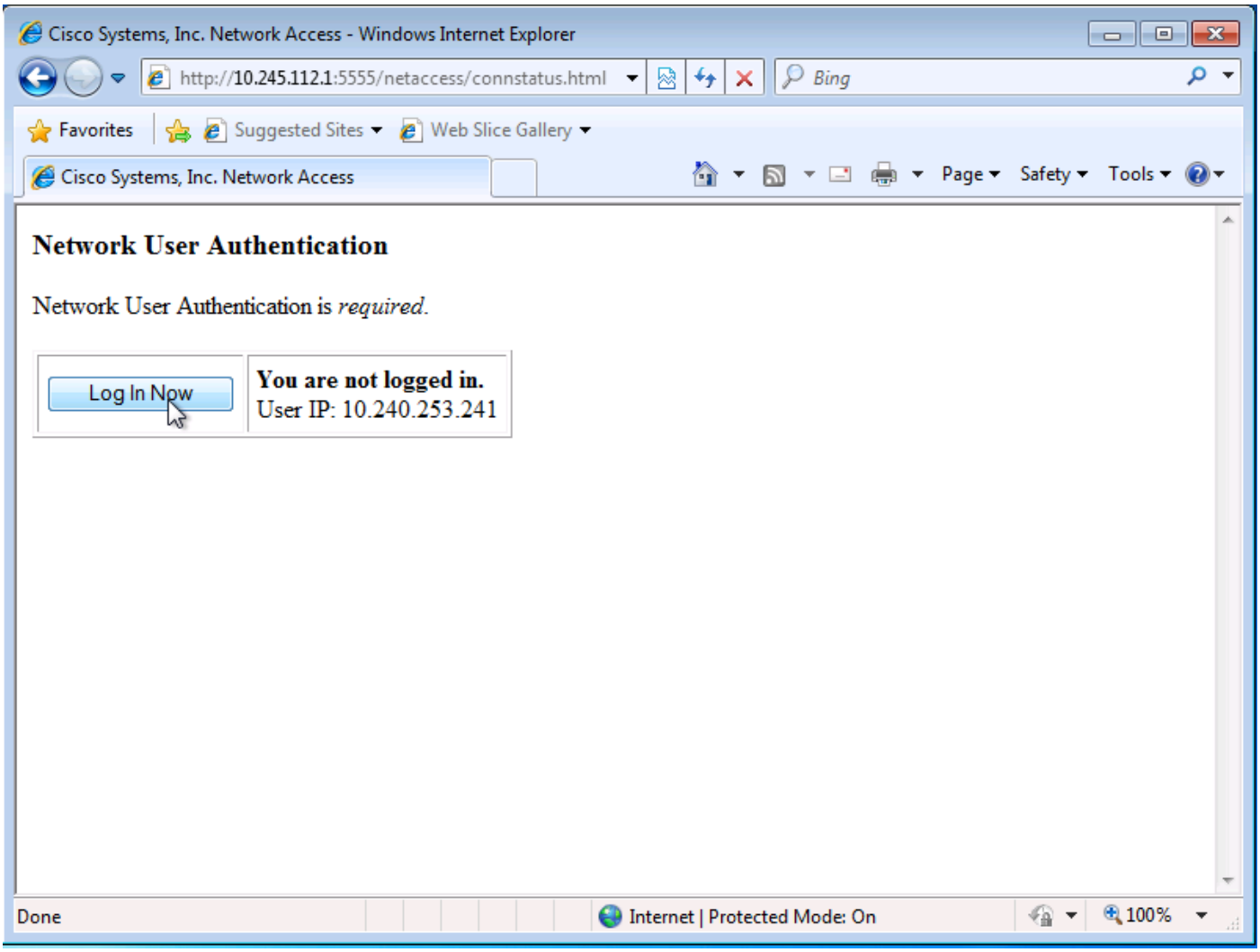
```
ciscoasa(config)# show asp table socket

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

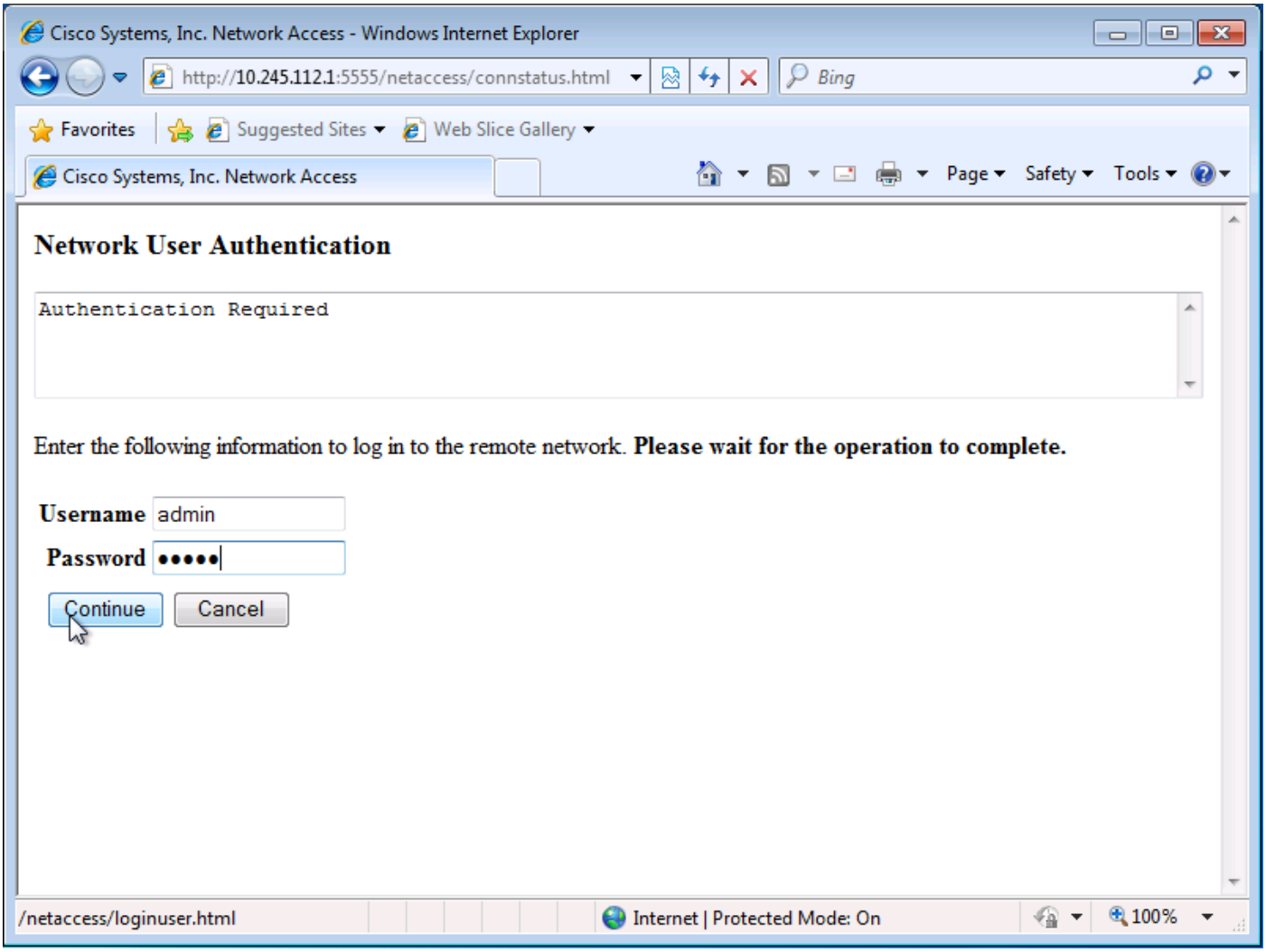
Nadat de ASA is geconfigureerd zoals hierboven wordt getoond, zal een poging tot verbinding door de ASA naar een externe host op TCP poort 3389 resulteren in een verbindingsontkenning. De gebruiker moet eerst voor TCP/389-verkeer authentiseren om te worden toegestaan.

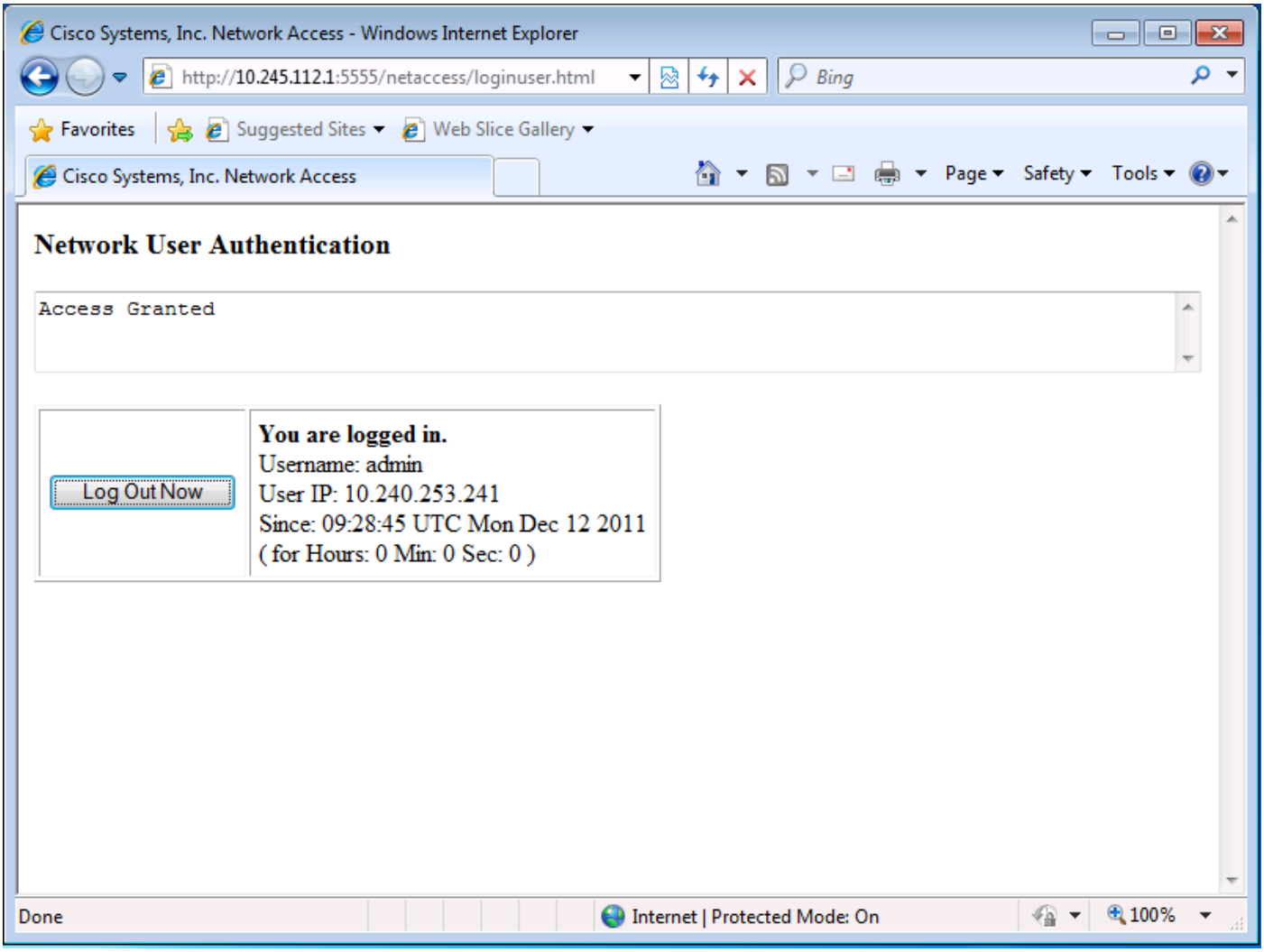
Directe authenticatie vereist dat de gebruiker direct naar de ASA bladert. Als u doorbladert naar http://<*asa_ip*>:<*port*>, wordt een fout van 404 teruggegeven omdat er geen webpagina bestaat bij de wortel van de ASA's webserver.



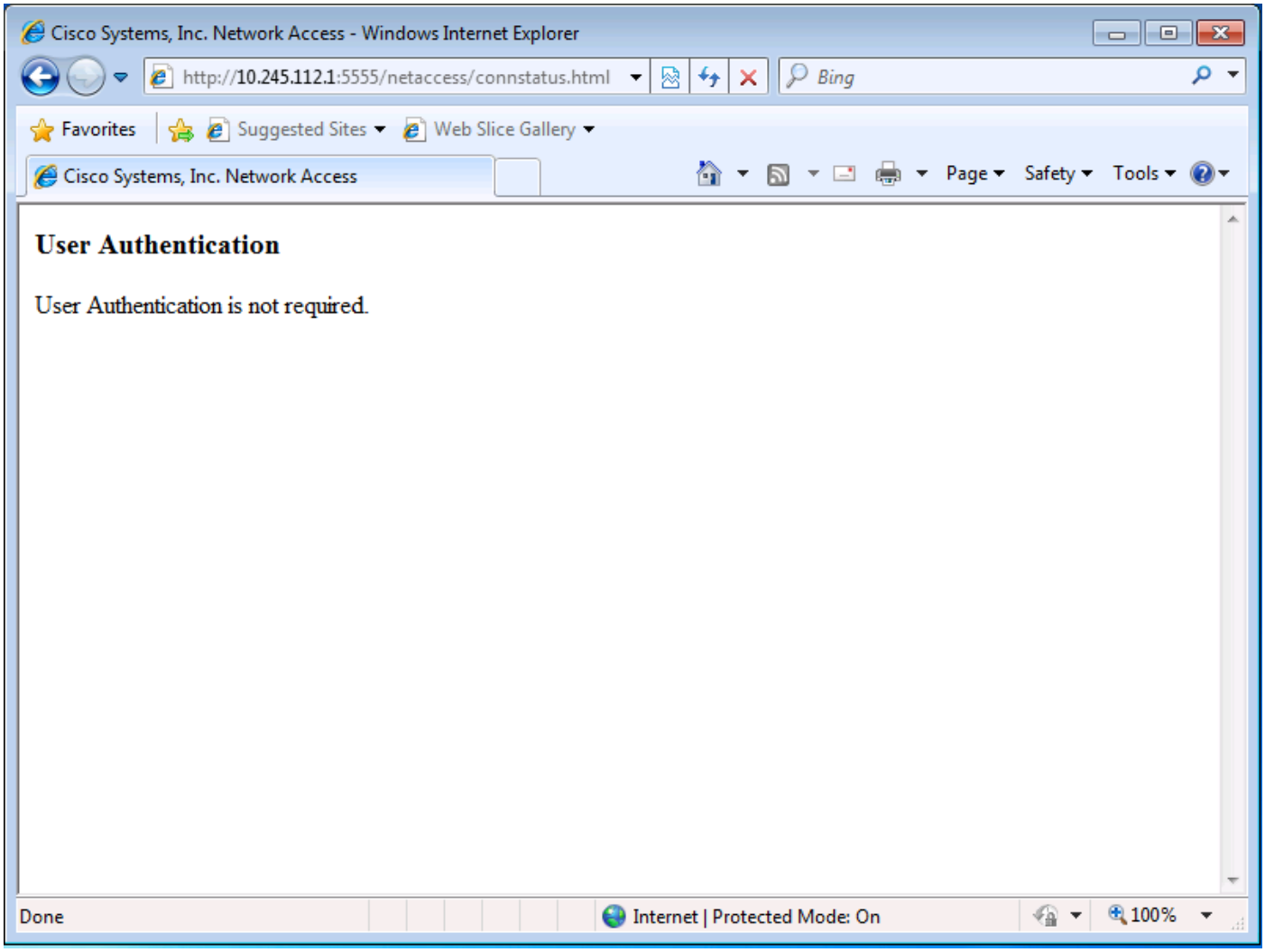
In plaats daarvan moet u rechtstreeks naar http://bladeren<*asa_ip*>:<*luisterer_port*>/netaccess/connstatus.html. Een loginpagina bevindt zich op deze URL waar u verificatiereferenties kunt bieden.




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 deze configuratie maakt het directe authenticatieverkeer deel uit van de autorisatie toegangslijst. Zonder deze access-control ingang kunt u een onverwacht bericht ontvangen, zoals *Gebruikersverificatie, gebruikersverificatie is niet vereist* wanneer u doorbladert naar http://<*asa_ip*>:<*lister_port*>/netaccess/connstatus.html.



Nadat u met succes authenticeert, kunt u via de ASA verbinding maken met een externe server op TCP/3389.