Konfigurationsbeispiel für Cut-Through- und Direct-ASA-Authentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Cut-Through- und Direkt-ASA-Authentifizierung konfiguriert wird.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf der Cisco Adaptive Security Appliance (ASA).

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

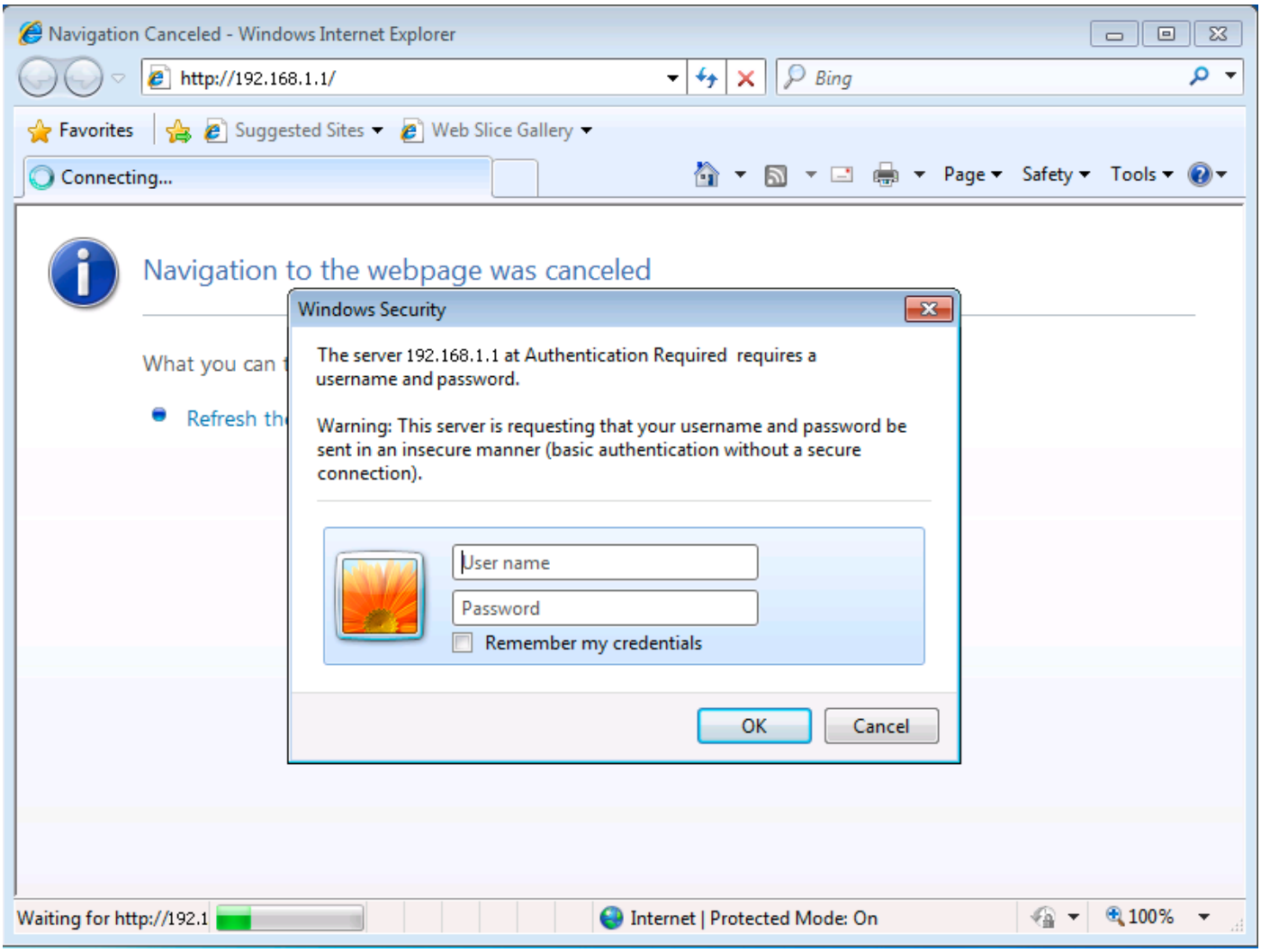
Durchschnittlich

Die Cut-Through-Authentifizierung wurde zuvor mit dem Befehl **aaa authentication include** konfiguriert. Der Befehl **aaa authentication match** wird nun verwendet. Datenverkehr, der eine Authentifizierung erfordert, wird in einer Zugriffsliste zugelassen, auf die der Befehl **aaa authentication match** verweist, wodurch der Host authentifiziert wird, bevor der angegebene Datenverkehr die ASA durchläuft.

Im Folgenden finden Sie ein Konfigurationsbeispiel für die Web-Datenverkehrsauthentifizierung:

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

Beachten Sie, dass diese Lösung funktioniert, da HTTP ein Protokoll ist, in das die ASA Authentifizierung einschleusen kann. Die ASA fängt HTTP-Datenverkehr ab und authentifiziert ihn über HTTP-Authentifizierung. Da die Authentifizierung inline eingegeben wird, wird im Webbrowser ein Dialogfeld für die HTTP-Authentifizierung angezeigt, wie in diesem Bild gezeigt:



Direkte Authentifizierung

Die direkte Authentifizierung wurde zuvor mit den **AAA-Authentifizierungsbefehlen** und den **virtuellen < Protokoll>**-Befehlen konfiguriert. Jetzt werden **aaa-Authentifizierungs-Übereinstimmungen** und **aaa-Authentifizierungslistener**-Befehle verwendet.

Für Protokolle, die keine native Authentifizierung unterstützen (d. h. Protokolle, die keine inline-Authentifizierung erfordern), kann eine direkte ASA-Authentifizierung konfiguriert werden. Standardmäßig überwacht die ASA keine Authentifizierungsanforderungen. Ein Listener kann auf einem bestimmten Port und einer bestimmten Schnittstelle mit dem Befehl **aaa authentication listener** konfiguriert werden.

Nachfolgend finden Sie ein Konfigurationsbeispiel, das TCP/3389-Datenverkehr über die ASA

zulässt, sobald ein Host authentifiziert wurde:

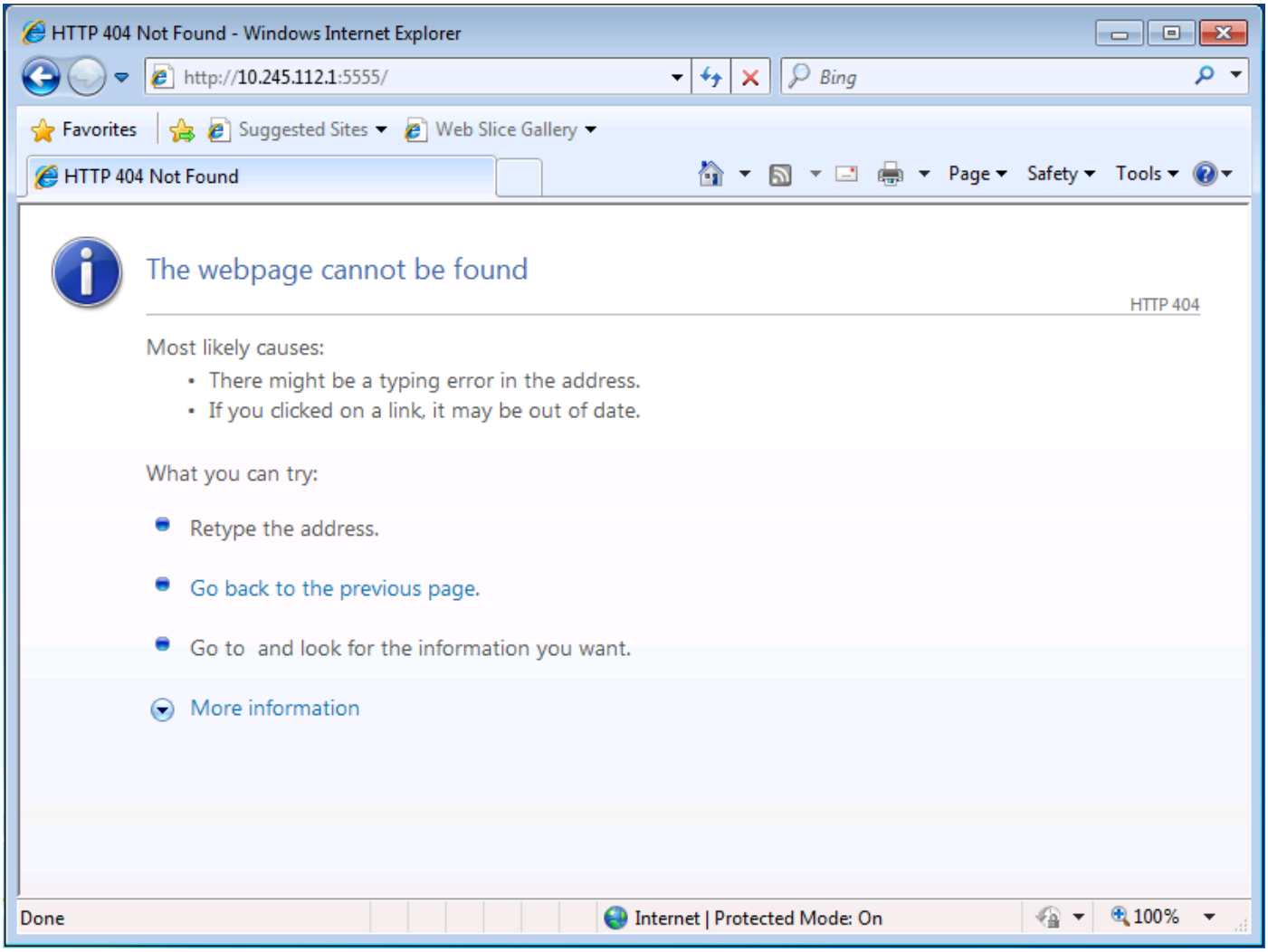
```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 3389
access-list authmatch permit tcp any host 10.245.112.1 eq 5555
aaa authentication match authmatch inside LOCAL
aaa authentication listener http inside port 5555
```

Beachten Sie die Portnummer, die vom Listener (TCP/5555) verwendet wird. Die Ausgabe des Befehls **show asp table socket** zeigt, dass die ASA jetzt Verbindungsanforderungen an diesen Port an der IP-Adresse überwacht, die der angegebenen (internen) Schnittstelle zugewiesen ist.

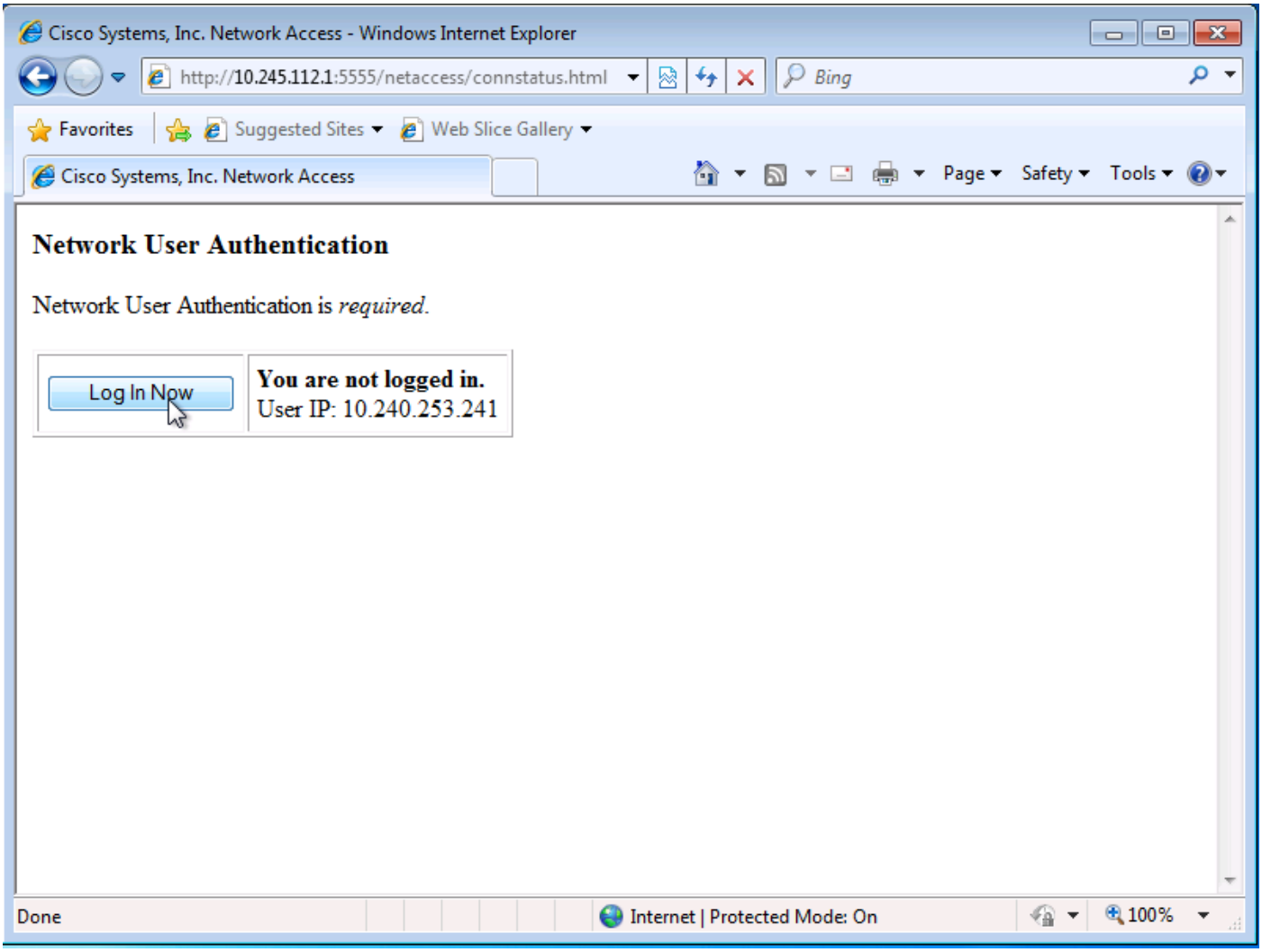
```
ciscoasa(config)# show asp table socket

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

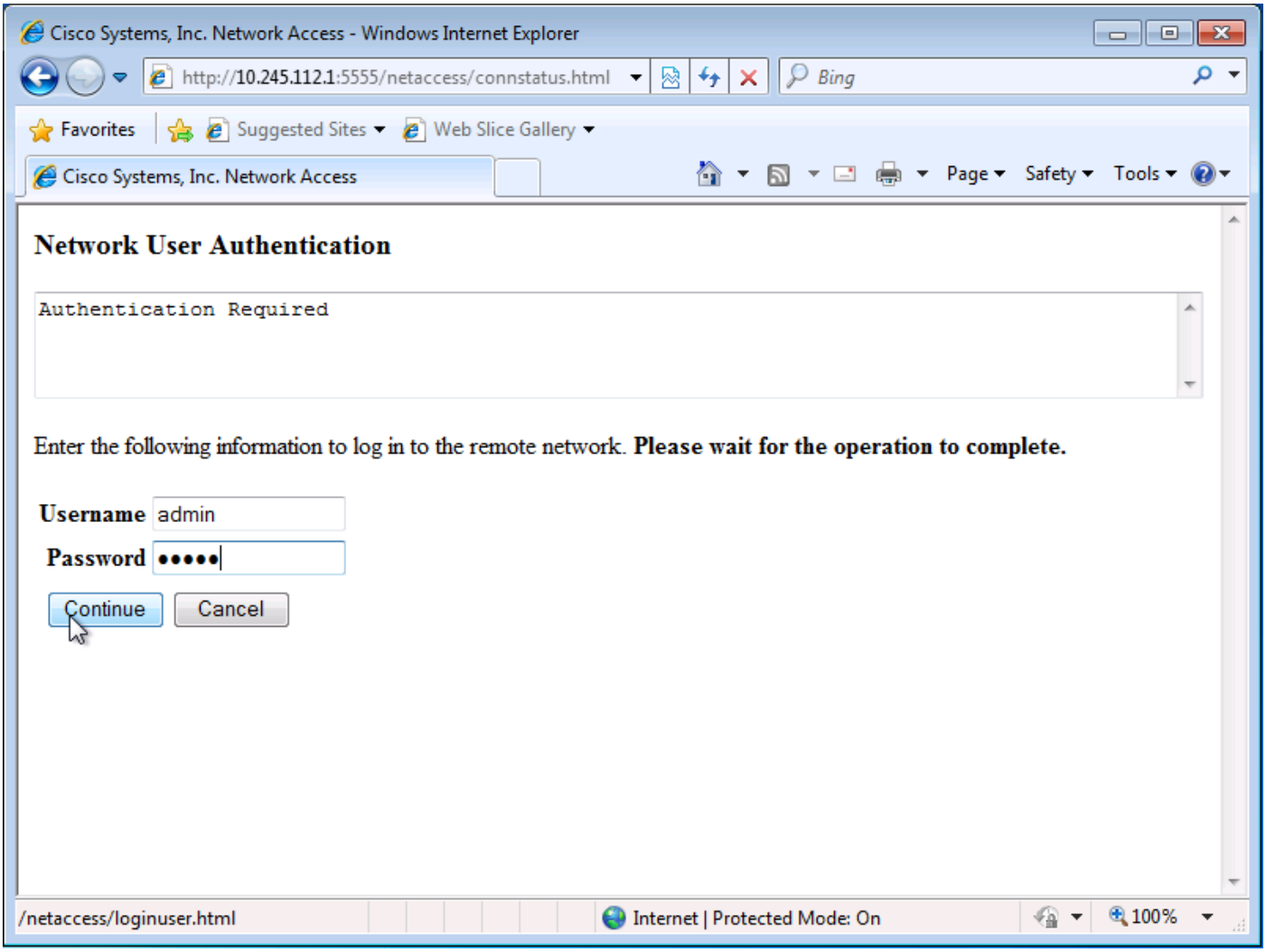
Nachdem die ASA wie oben gezeigt konfiguriert wurde, führt ein Verbindungsversuch über die ASA mit einem externen Host am TCP-Port 3389 zu einer Verbindungsverweigerung. Der Benutzer muss sich zunächst authentifizieren, damit TCP/3389-Datenverkehr zugelassen werden kann.

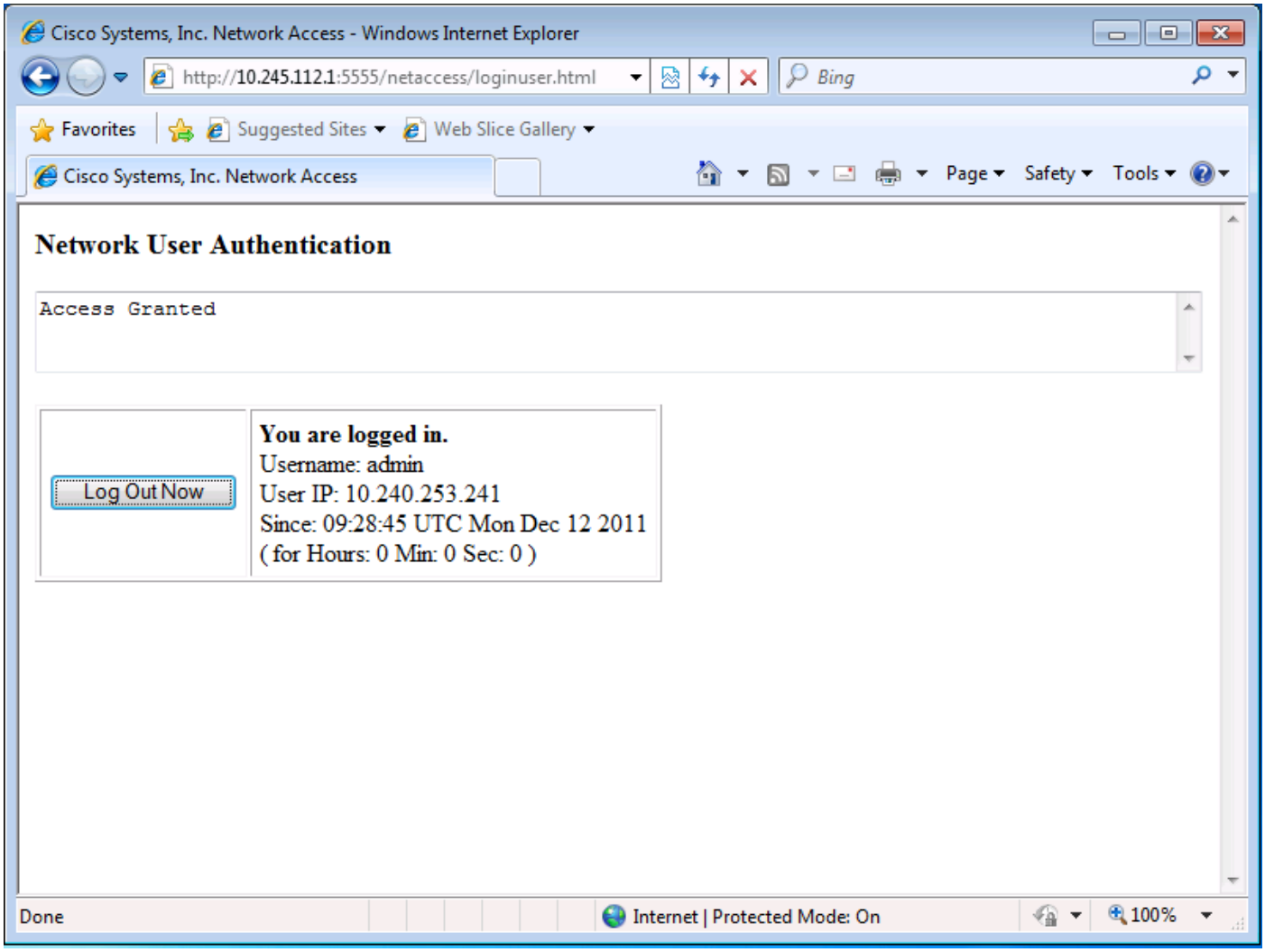
Bei der direkten Authentifizierung muss der Benutzer direkt zur ASA navigieren. Wenn Sie zu http://<*asa_ip*>:<*port*> wechseln, wird ein 404-Fehler zurückgegeben, da keine Webseite im Root des ASA-Webservers vorhanden ist.



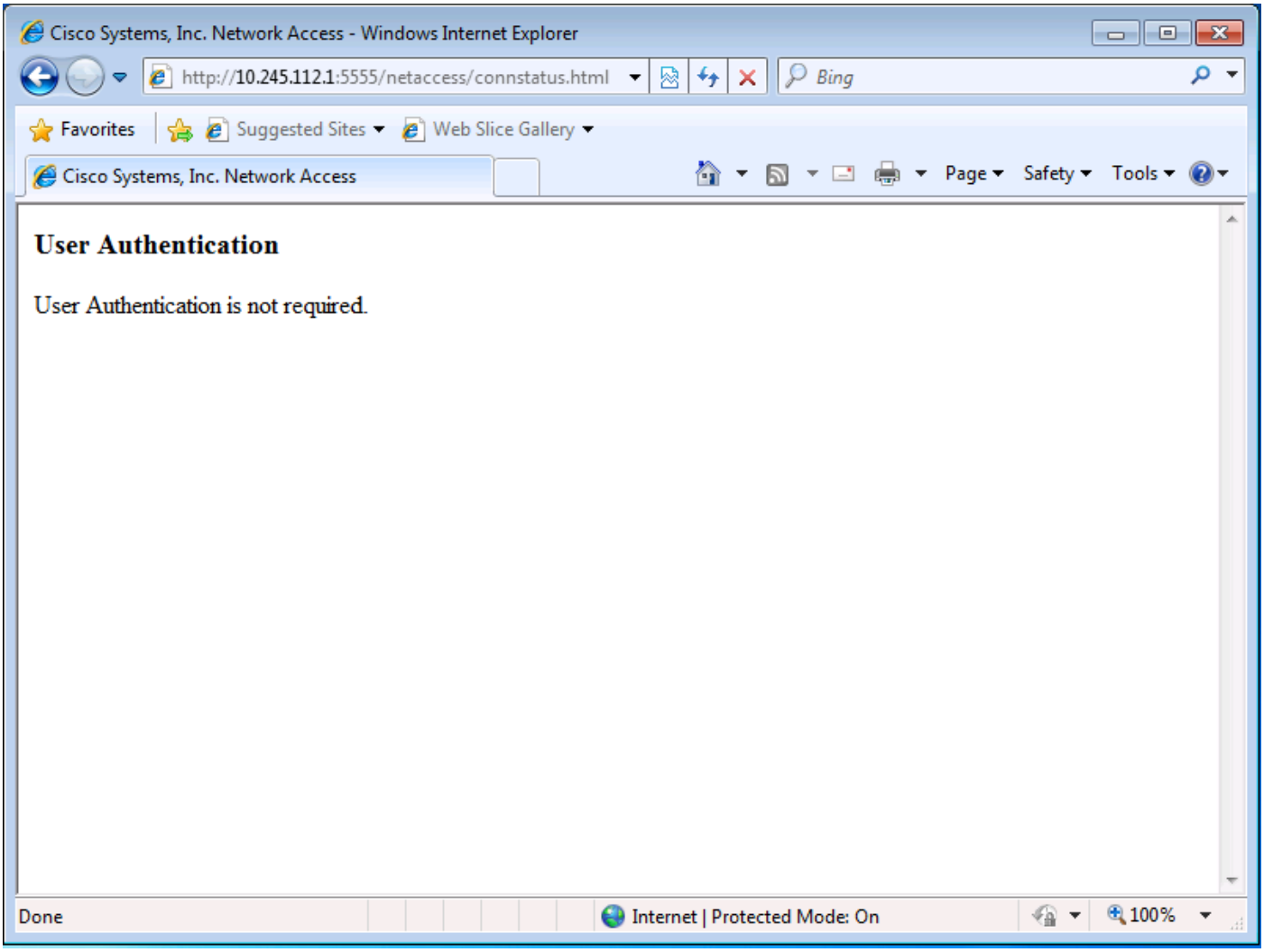
Stattdessen müssen Sie direkt zu http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html navigieren. Eine Anmeldeseite befindet sich an dieser URL, über die Sie Authentifizierungsanmeldeinformationen angeben können.


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%



In dieser Konfiguration ist der Datenverkehr für die direkte Authentifizierung Teil der Zugriffsliste für authentifiziertes Kennwort. Ohne diesen Zugriffskontrolleintrag erhalten Sie möglicherweise eine unerwartete Meldung, z. B. *Benutzerauthentifizierung,* wenn Sie *die* Website http://<*asa_ip*>:<*listener_port*>/netaccess/connstatus.html aufrufen.



Nachdem Sie sich erfolgreich authentifiziert haben, können Sie über die ASA eine Verbindung zu einem externen Server über TCP/3389 herstellen.