컷스루 및 직접 ASA 인증 컨피그레이션 예

목차

소개

이 문서에서는 컷스루 및 직접 ASA 인증을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco ASA(Adaptive Security Appliance)를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

컷스루

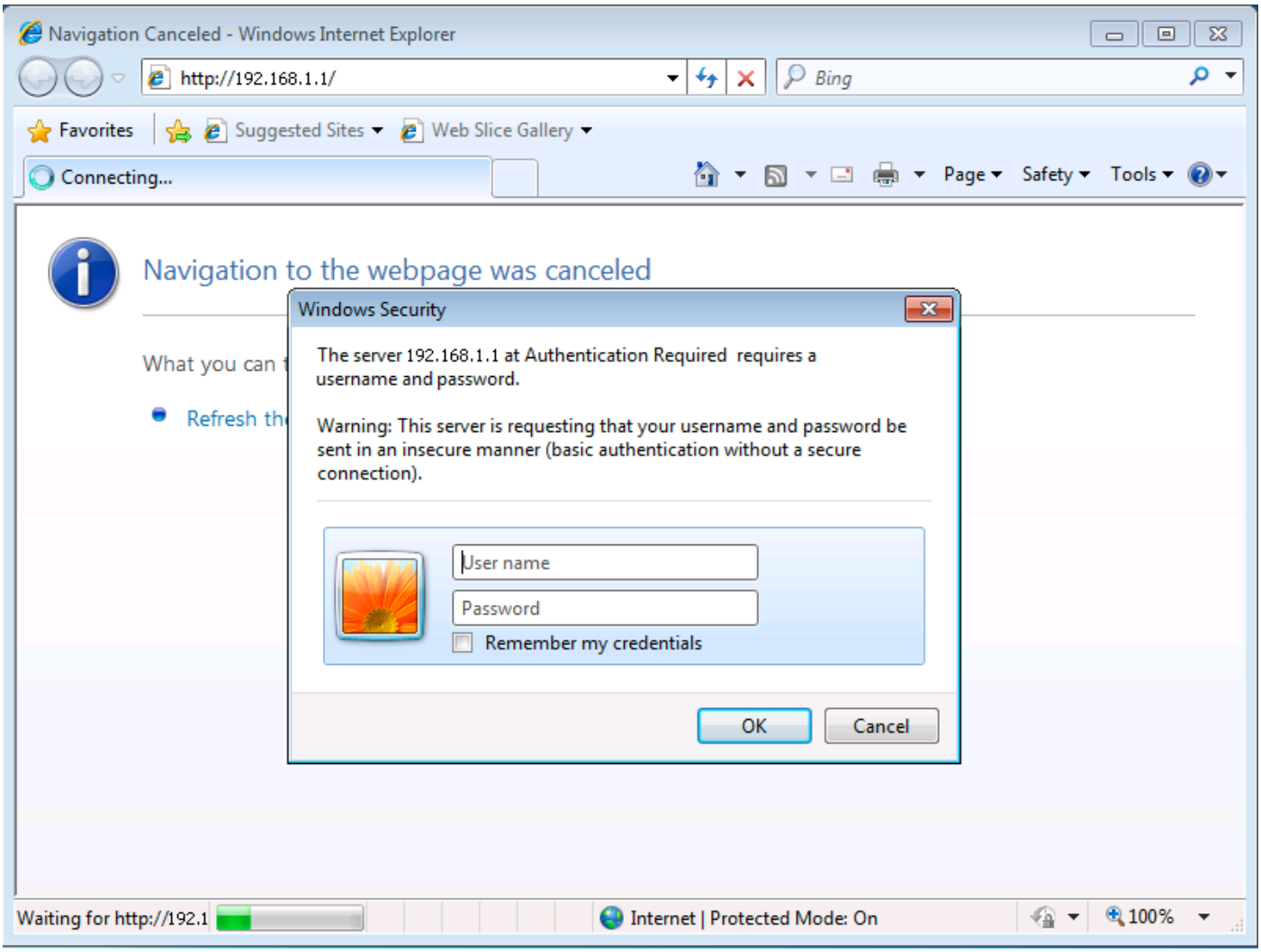
컷스루 인증은 이전에 aaa authentication include 명령을 사용하여 **구성되었습니다**.이제 aaa **authentication match** 명령이 사용됩니다.인증이 필요한 트래픽은 **aaa authentication match** 명령에서 참조하는 액세스 목록에서 허용되며, 이 경우 지정된 트래픽이 ASA를 통해 허용되기 전에 호스트가 인증됩니다.

다음은 웹 트래픽 인증을 위한 컨피그레이션 예입니다.

```
username cisco password cisco privilege 15
access-list authmatch permit tcp any any eq 80
```

```
aaa authentication match authmatch inside LOCAL
```

이 솔루션은 HTTP가 ASA에서 인증을 삽입할 수 있는 프로토콜이므로 작동합니다.ASA는 HTTP 트래픽을 인터셉트하고 HTTP 인증을 통해 이를 인증합니다.인증이 인라인으로 삽입되므로 HTTP 인증 대화 상자가 다음 이미지에 표시된 대로 웹 브라우저에 나타납니다.



직접 인증

직접 인증은 이전에 aaa **authentication include** 및 **virtual < protocol>** 명령**으로** 구성되었습니다.이제 aaa **authentication match** 및 **aaa authentication listener** 명령이 사용됩니다.

기본적으로 인증을 지원하지 않는 프로토콜(즉, 인라인 인증 챌린지를 가질 수 없는 프로토콜)의 경우 직접 ASA 인증을 구성할 수 있습니다.기본적으로 ASA는 인증 요청을 수신하지 않습니다.리스너는 aaa authentication listener 명령을 사용하여 특정 포트 및 인터페이스에서 구성할 수 있습니다 .

다음은 호스트가 인증되면 ASA를 통해 TCP/3389 트래픽을 허용하는 컨피그레이션 예입니다.

```
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
```

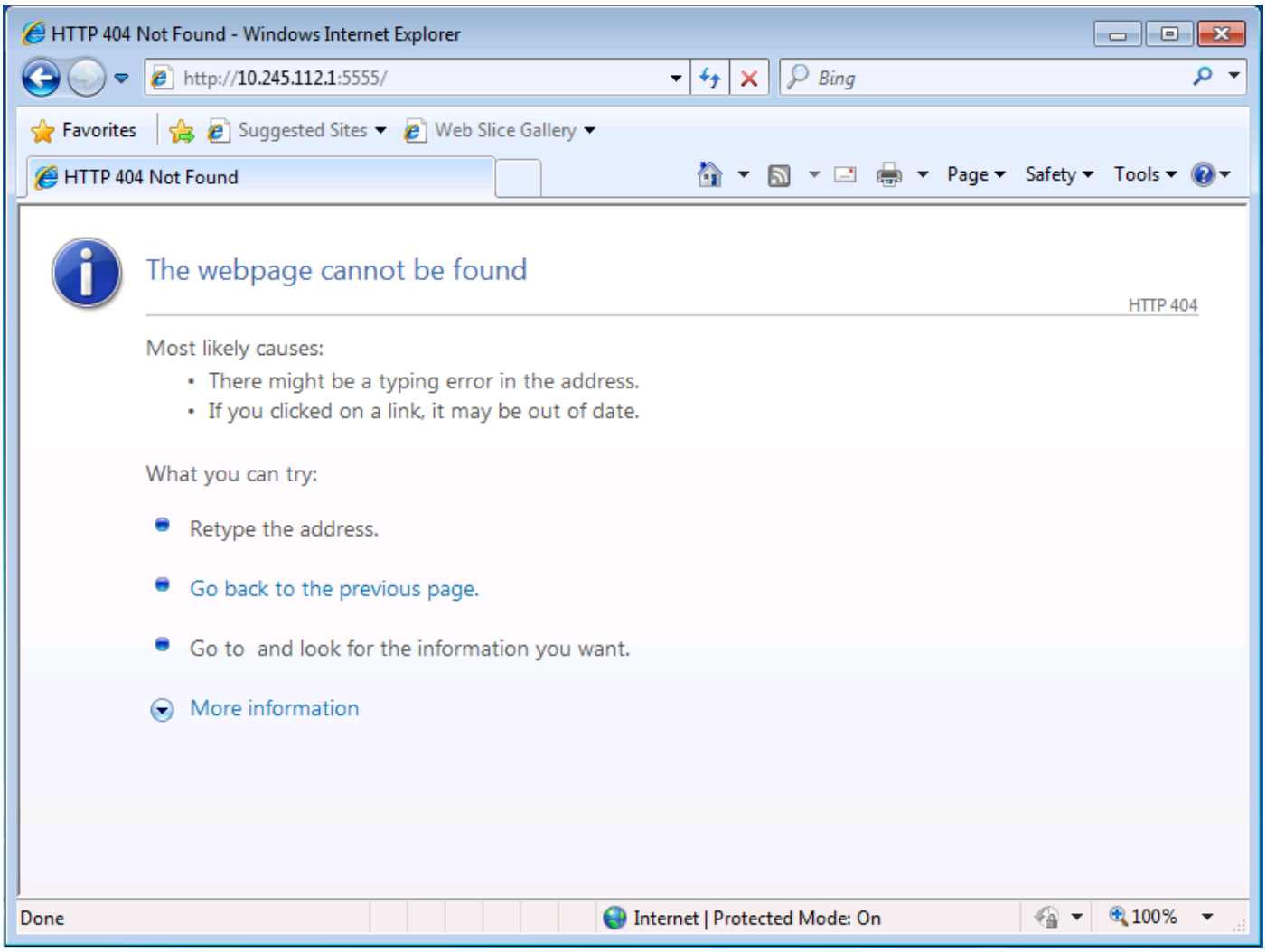
리스너가 사용하는 포트 번호(TCP/5555)를 확인합니다. show **asp table socket** 명령 출력은 ASA가 이제 지정된(내부) 인터페이스에 할당된 IP 주소에서 이 포트에 대한 연결 요청을 수신함을 보여줍

니다.

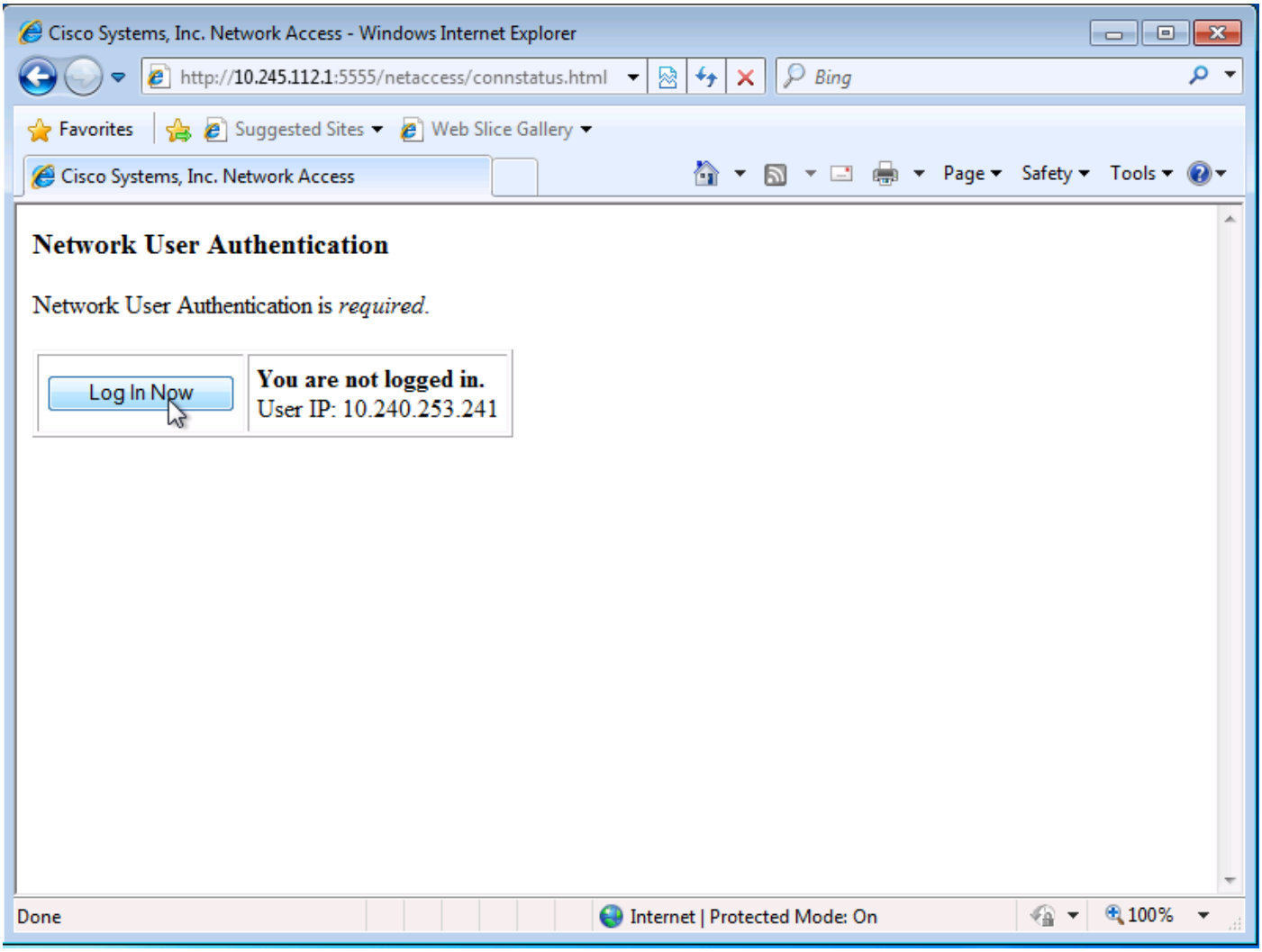
```
ciscoasa(config)# show asp table socket

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

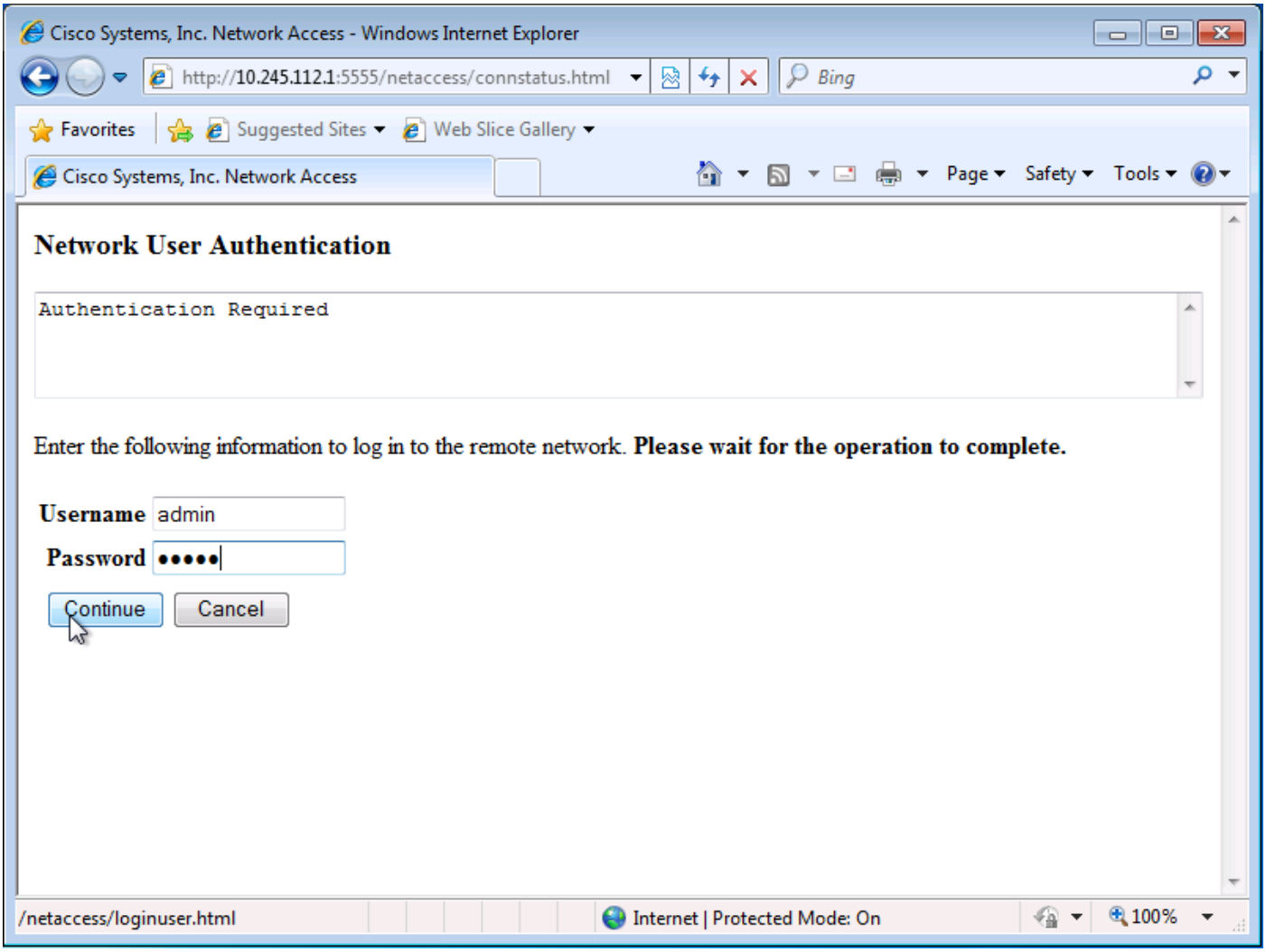
위에 표시된 대로 ASA를 구성한 후 TCP 포트 3389의 외부 호스트에 ASA를 통해 연결을 시도하면 연결 거부가 발생합니다.사용자는 먼저 TCP/3389 트래픽에 대해 인증해야 허용됩니다.

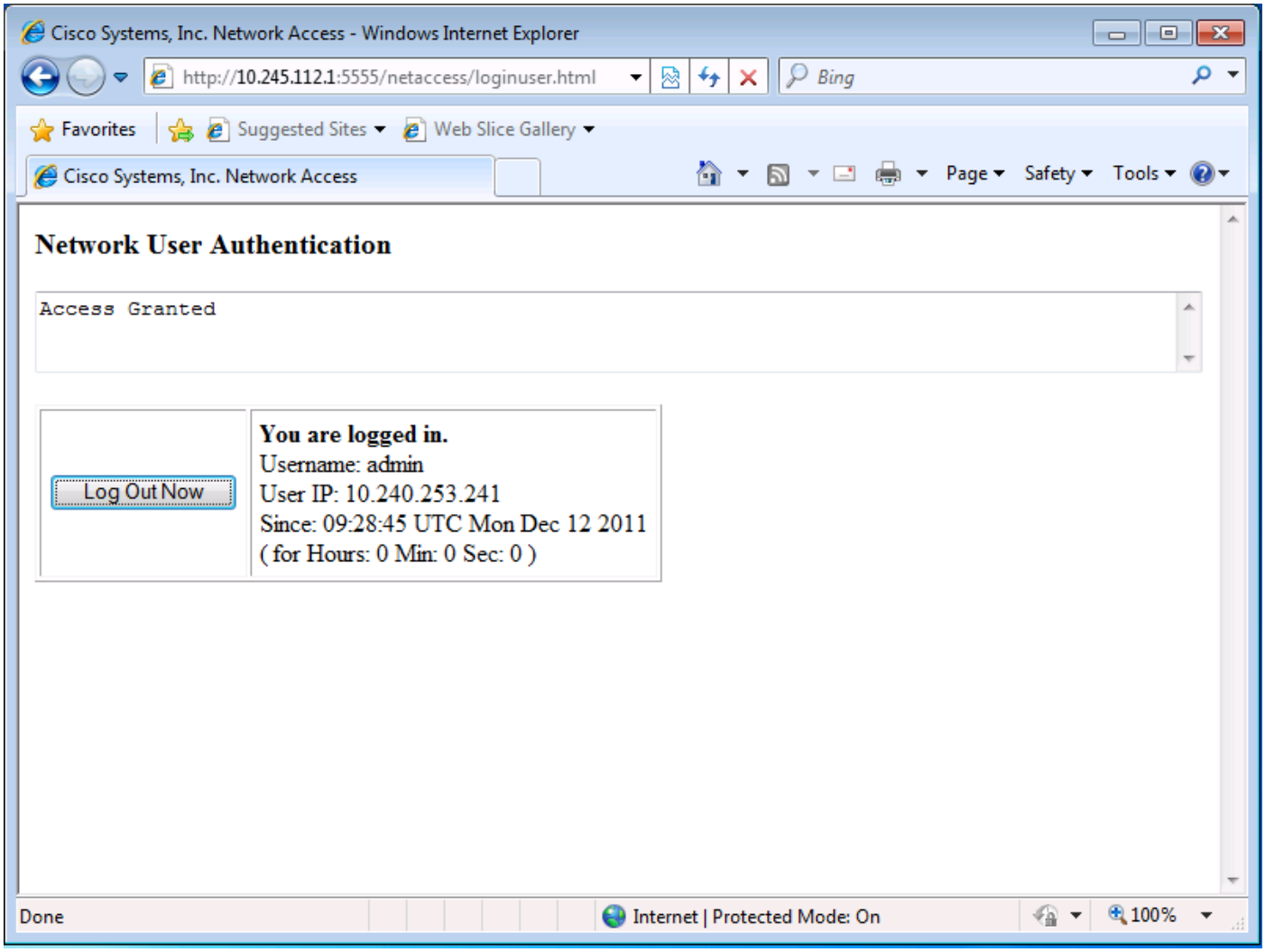
직접 인증을 수행하려면 사용자가 ASA로 직접 이동해야 합니다.http://<*asa_ip*>:<*port*>로 이동하면 ASA 웹 서버의 루트에 웹 페이지가 없으므로 404 오류가 반환됩니다.



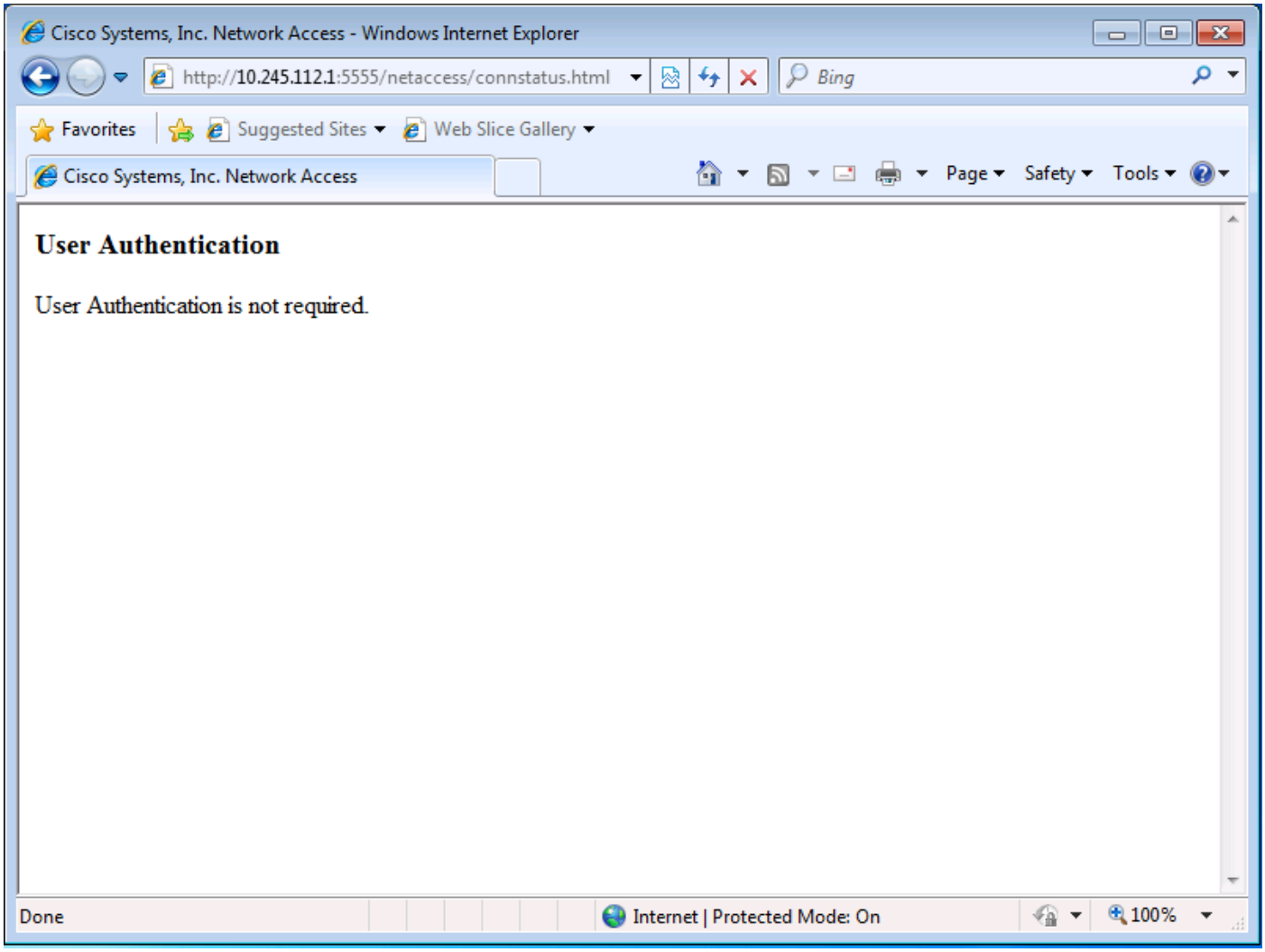
대신 http://<*asa_ip*>:<listener_*port*>/netaccess/connstatus.html으로 직접 찾아보아야 합니다.로그인 페이지는 인증 자격 증명을 제공할 수 있는 이 URL에 있습니다.


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%



이 컨피그레이션에서는 직접 인증 트래픽이 authmatch access-list의 일부입니다.이 액세스 제어 항목이 없으면 http://<*asa_ip*>:<listener_port>/netaccess/connstatus.html로 이동할 때 *User Authentication, User Authentication is not required(사용자 인증, 사용자 인증 필요 없음)*와 같은 예기치 않은 메시지를 받을 수 있습니다.



성공적으로 인증하면 ASA를 통해 TCP/3389의 외부 서버에 연결할 수 있습니다.