

カットスルーと直接の ASA 認証の設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[カットスルー](#)

[直接認証](#)

概要

このドキュメントでは、カットスルーと直接 ASA 認証を設定する方法について説明します。

前提条件

要件

このドキュメントに特有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco Adaptive Security Appliance (ASA) に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

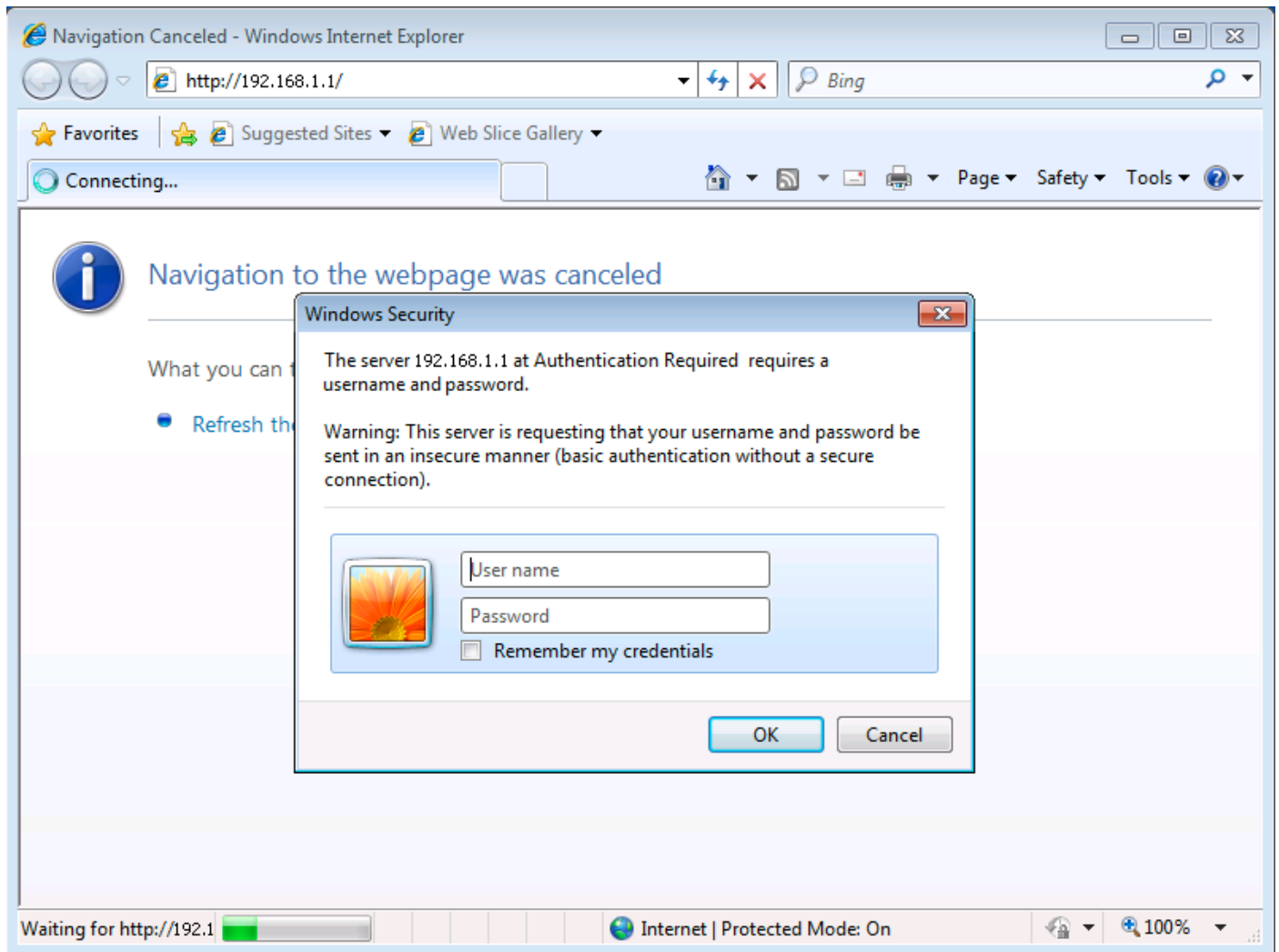
カットスルー

カットスルー認証を設定するには、以前は `aaa authentication include` コマンドが使用されていました。現在は、`aaa authentication match` コマンドを使用するようになっています。`aaa authentication match` コマンドでアクセス リストを参照し、認証を必要とするトラフィックをアクセス リスト内で許可します。これにより、指定されたトラフィックに ASA の経路が許可される前に、ホストの認証が行われるようになります。

以下に、Web トラフィック認証の設定例を示します。

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

この解決法が有効となる理由は、プロトコルとして HTTP が使用されているためです。プロトコルが HTTP であれば、ASA は認証を注入できます。ASA は HTTP トラフィックをインターセプトし、HTTP 認証による認証を行います。認証はインラインで注入されているため、HTTP 認証ダイアログボックスが Web ブラウザに表示されます (以下の図を参照)。



直接認証

直接認証を設定するには、以前は `aaa authentication include` および `virtual <protocol>` コマンドが使用されていました。現在は、`aaa authentication match` および `aaa authentication listener` コマンドを使用するようになっています。

認証をネイティブにサポートしていないプロトコル (つまり、認証チャレンジをインラインで使用できないプロトコル) については、直接認証を設定できます。デフォルトでは、ASA は認証要求をリッスンしません。`aaa authentication listener` コマンドを使用することで、特定のポートとインターフェイスにリスナーを設定できます。

以下に示す設定例では、ホストの認証が完了すると、TCP/3389 トラフィックに ASA の経路が許可されます。

```
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
```

リスナーで使用しているポート番号 (TCP/5555) に注意してください。 `show asp table socket` コマンドの出力に、IP アドレスが特定の (内部) インターフェイスに割り当てられたこのポートへの接続要求を ASA がリッスンするようになったことが示されます。

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

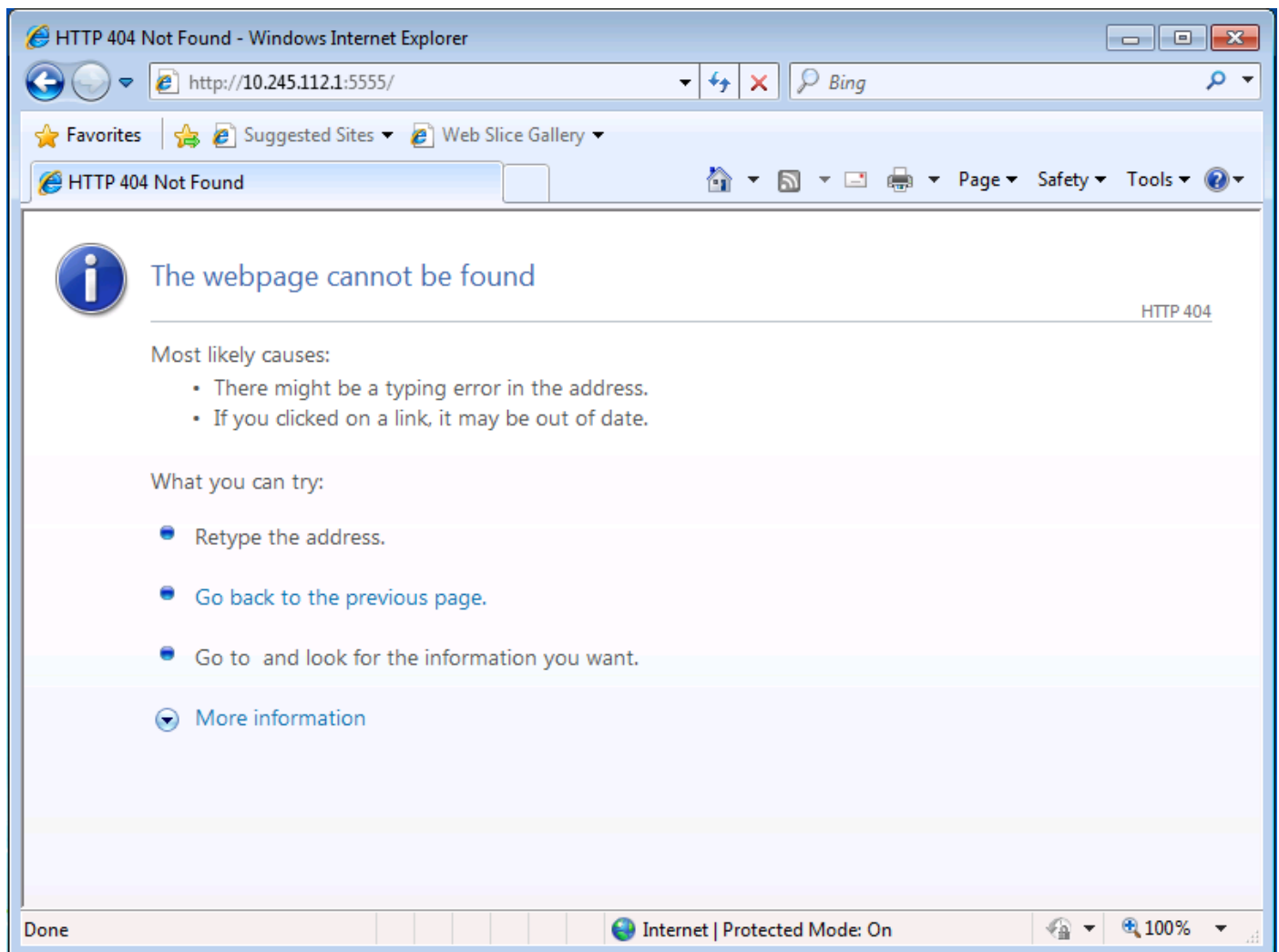
```
Protocol Socket Local Address Foreign Address State
```

```
TCP 000574cf 10.245.112.1:5555 0.0.0.0:* LISTEN
```

```
ciscoasa(config)#
```

ASA が上記のように設定されると、TCP ポート 3389 上での ASA を介した外部ホストへの接続試行は拒否される結果になります。TCP/3389 トラフィックを許可するには、まずその前に認証が必要です。

直接認証では、ユーザが ASA を直接参照する必要があります。 `http://<asa_ip>:<port>` を参照すると、ASA の Web サーバのルートに Web ページが存在しないため、404 エラーが返されます。



代わりに、 `http://<asa_ip>:<listener_port>/netaccess/connstatus.html` を直接参照する必要があります。この URL に、認証クレデンシャルを入力できるログイン ページがあります。

Network User Authentication

Network User Authentication is *required*.

Log In Now	You are not logged in. User IP: 10.240.253.241
----------------------------	--

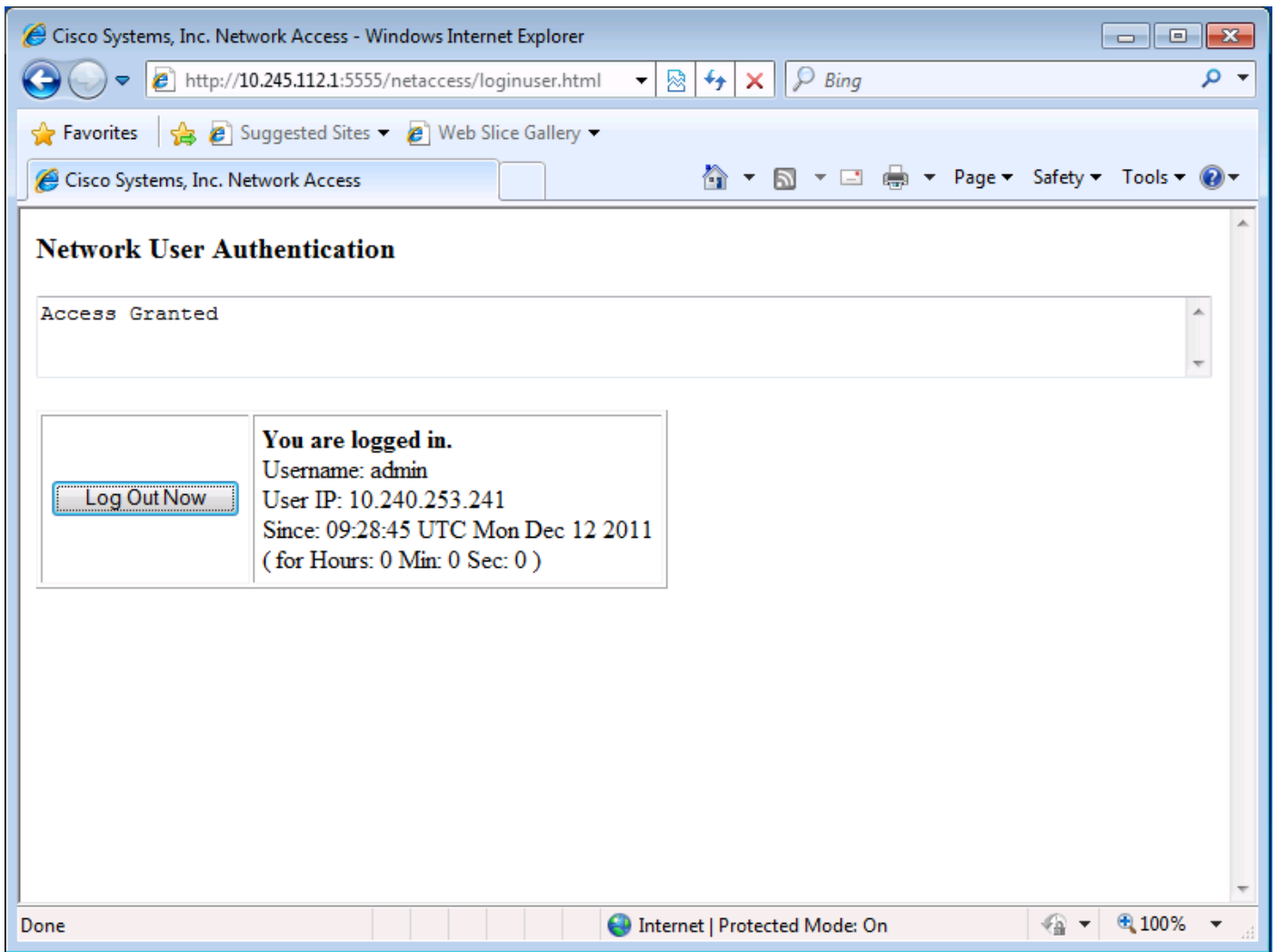
Network User Authentication

Authentication Required

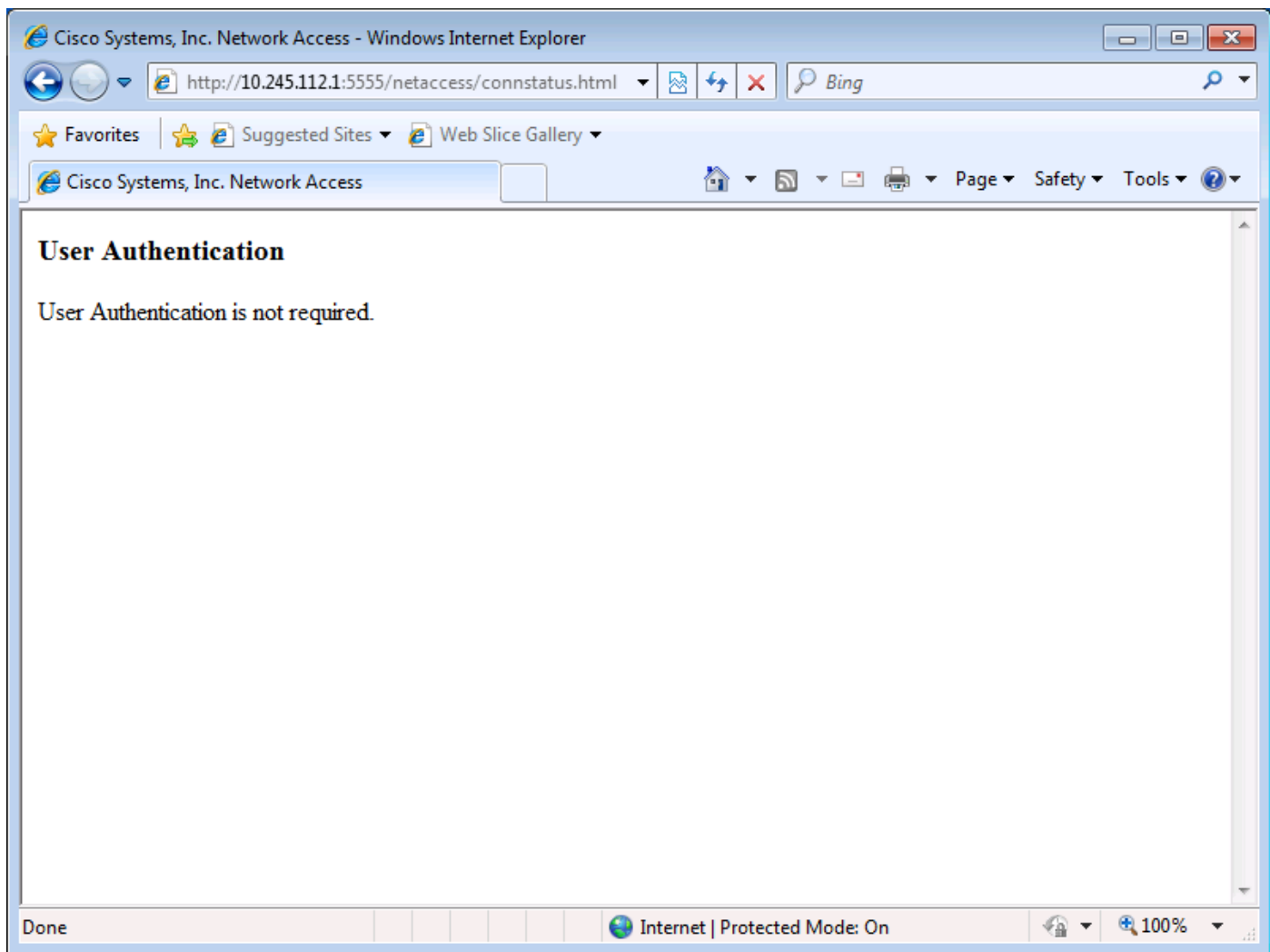
Enter the following information to log in to the remote network. **Please wait for the operation to complete.**

Username

Password



この設定では、直接認証のトラフィックが authmatch アクセス リストに含まれています。このアクセス制御エントリがない場合、`http://<asa_ip>:<listener_port>/netaccess/connstatus.html`をブラウザすると、*User Authentication*, *User Authentication is not required*などの予期しないメッセージが表示される場合があります。



認証が成功すると、TCP/3389 で ASA を介して外部サーバに正常に接続できるようになります。