Configuring Captive Portal Authentication (CLI Procedure)

Configure captive portal authentication (hereafter referred to as captive portal) on an EX Series switch so that users connected to the switch are authenticated before being allowed to access the network. When the user requests a webpage, a login page is displayed that requires the user to input a username and password. Upon successful authentication, the user is allowed to continue with the original page request and subsequent access to the network.

Before you begin, be sure you have:

- Performed basic bridging and VLAN configuration on the switch. See Example: Setting Up Basic Bridging and a VLAN for an EX Series Switch.
- Generated an SSL certificate and installed it on the switch. See Generating SSL Certificates to Be Used for Secure Web Access.
- Configured basic access between the EX Series switch and the RADIUS server. See Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch.
- Designed your captive portal login page. See Designing a Captive Portal Authentication Login Page on an EX Series Switch.

This topic includes the following tasks:

Configuring Secure Access for Captive Portal

To configure secure access for captive portal:

1. Associate the security certificate with the Web server and enable HTTPS on the switch:

```
[edit]
user@switch# set system services web-management https local-certificate
my-signed-cert
```

NOTE: You can enable HTTP instead of HTTPS, but we recommend HTTPS for security purposes.

2. Configure captive portal to use HTTPS:

```
[edit]
user@switch# set services captive-portal secure-authentication https
```

Enabling an Interface for Captive Portal

To enable an interface for use with captive portal authentication:

```
[edit]
user@switch# set services captive-portal interface ge-0/0/10
```

Configuring Bypass of Captive Portal Authentication

You can allow specific clients to bypass captive portal authentication:

```
[edit]
user@switch# set ethernet-switching-options authentication-whitelist
00:10:12:e0:28:22
```

NOTE: Optionally, you can use set ethernet-switching-options authentication-whitelist 00:10:12:e0:28:22 interface ge-0/0/10.0 to limit the scope to the interface.

If the MAC address of the client that you want to configure for authentication bypass has already been learned on the interface, you must clear it using the clear captive-portal interface *interface-name*before adding it to the whitelist. Otherwise the new entry for the MAC address will not be added to the ethernet switching table and the authentication bypass will not be allowed.

Related Topics

- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Understanding Captive Portal Authentication

Published: 2010-01-15