

Konfigurationsbeispiel für Webauthentifizierungsproxy

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Konfigurieren des WLC](#)

[Konfigurieren der PAC-Datei](#)

[Vorauthentifizierungs-ACL erstellen](#)

[Schnellreparatur: Webbrowser konfigurieren](#)

[Überprüfen](#)

[Fehlerbehebung](#)

Einführung

In diesem Dokument wird beschrieben, wie Sie die Webauthentifizierung konfigurieren, um mit einer Proxy-Konfiguration zu arbeiten.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundlegende Konfiguration des Wireless LAN Controllers
- Webauthentifizierungs-Sicherheit

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco Wireless LAN Controller Version 7.0 und höher.

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.

Konfigurieren

Netzwerkadministratoren, die über einen Proxyserver im Netzwerk verfügen, senden zunächst den

Webdatenverkehr an den Proxyserver, der den Datenverkehr dann an das Internet weiterleitet. Verbindungen zwischen Client und Proxyserver können einen anderen TCP-Port als Port 80 für die Kommunikation verwenden. Dieser Port ist normalerweise TCP-Port 3128 oder 8080. Standardmäßig überwacht die Webauthentifizierung nur Port 80. Wenn ein HTTP GET den Computer verlässt, wird es an den Proxyport gesendet, aber vom Controller verworfen.

In diesem Abschnitt wird beschrieben, wie Sie die Webauthentifizierung konfigurieren, um mit einer Proxy-Konfiguration zu arbeiten:

1. Konfigurieren Sie den Cisco Wireless LAN Controller (WLC), um den Proxyport anzuhören.
2. Konfigurieren Sie die Proxy-Datei für die automatische Konfiguration (PAC), um die virtuelle IP-Adresse direkt zurückzugeben.
3. Erstellen Sie eine ACL (Preauthentication Access Control List), damit der Client die PAC-Datei vor der Webauthentifizierung herunterladen kann.

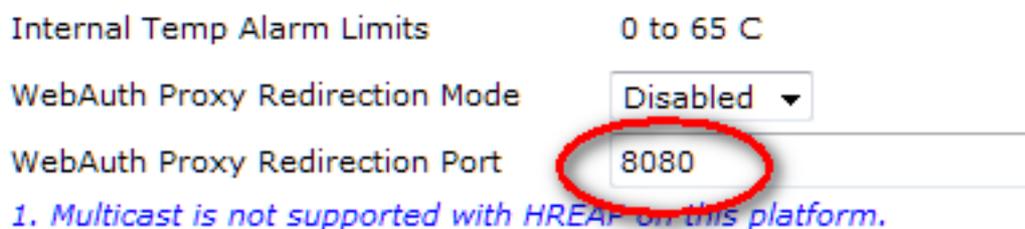
Als schnelle Lösung können Sie den Webbrowser manuell konfigurieren, um 192.0.2.1 zurückzugeben.

Details zu jedem dieser Prozesse finden Sie in den nächsten Unterabschnitten.

Konfigurieren des WLC

In diesem Verfahren wird beschrieben, wie Sie den Port ändern, den der Controller auf dem Port abhört, auf dem der Proxyserver wartet.

1. Navigieren Sie zur Seite **Controller > Allgemein**.



| | |
|--------------------------------|------------|
| Internal Temp Alarm Limits | 0 to 65 C |
| WebAuth Proxy Redirection Mode | Disabled ▼ |
| WebAuth Proxy Redirection Port | 8080 |

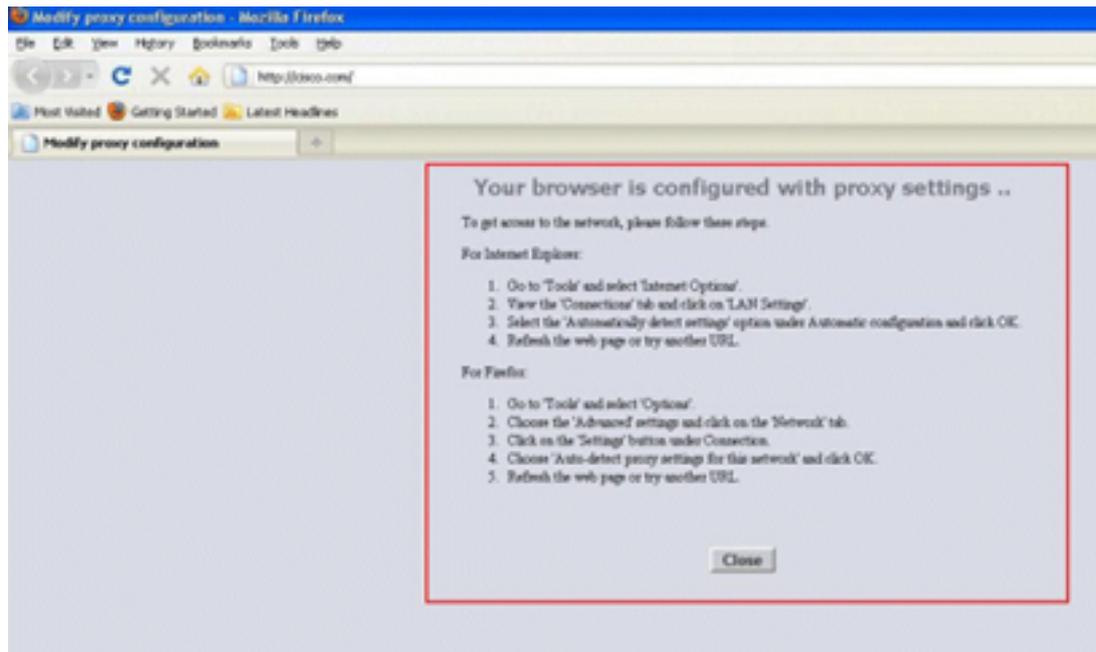
1. Multicast is not supported with HREAP on this platform.

2. Geben Sie im Feld WebAuth Proxy Redirection Port (WebAuth-Proxy-Umleitungsport) den Port ein, an dem der WLC die Client-Umleitung überwachen soll.
3. Wählen Sie in der Dropdown-Liste WebAuth Proxy Redirection Mode (WebAuth-Proxyumleitungsmodus) die Option Disabled (Deaktiviert) oder Enabled (Aktiviert) aus:

Wenn Sie **Disabled (Deaktiviert)** auswählen, wird den Clients die normale Webseite zur Authentifizierung für Passthrough oder Authentifizierung angezeigt. Wenn Sie also einen Proxy verwenden, müssen Sie alle Clientbrowser so konfigurieren, dass der Proxy für 192.0.2.1 (oder eine andere virtuelle IP-Adresse, die der WLC verwendet) nicht verwendet wird. Siehe [Webbrowser konfigurieren](#).

Wenn Sie **Enabled (Aktiviert)** auswählen, überwacht der WLC standardmäßig die Ports 80, 8080 und 3128, sodass Sie diese Ports nicht im Textfeld WebAuth Proxy Redirection Port (WebAuth-Proxy-Umleitungsport) eingeben müssen. Wenn ein Client eine HTTP GET-Schnittstelle an diese Ports sendet, wird ein Bildschirm angezeigt, in dem er aufgefordert

wird, seine Proxy-Einstellungen automatisch zu ändern.



4. Speichern Sie die Konfiguration.

5. Starten Sie den Controller neu.

Geben Sie zusammenfassend eine Portnummer in WebAuth Proxy Redirection Port ein, um den Port zu definieren, den der WLC überwacht. Wenn der Umleitungsmodus aktiviert ist, leitet er den Client zum Bildschirm für die Proxyeinstellungen um und erwartet, dass er dynamisch eine Web Proxy Auto-Discovery (WPAD)- oder PAC-Datei für die automatische Proxy-Konfiguration überträgt. Bei Deaktivierung wird der Client zur normalen Webseite für die Authentifizierung umgeleitet.

Konfigurieren der PAC-Datei

Die virtuelle IP-Adresse des WLC muss 'direkt' zurückgegeben werden, damit die Web-Auth Benutzer korrekt authentifizieren kann. Direct bedeutet, dass der Proxy-Server nicht auf die Anforderung verweist, und der Client über die Berechtigung verfügt, direkt auf die IP-Adresse zuzugreifen. Dies wird in der Regel vom Proxy-Server-Administrator auf dem Proxyserver in der WPAD- oder PAC-Datei konfiguriert. Dies ist eine Beispielkonfiguration für eine PAC-Datei:

```
function FindProxyForURL(url, host) {
    // our local URLs from the domains below example.com don't need a proxy:
    if (shExpMatch(host, "*.example.com"))
    if (shExpMatch(host, "192.0.2.1"))    <-- (Line states return 1.1.1 directly)
    {
        return "DIRECT";
    }

    // URLs within this network are accessed through
    // port 8080 on fastproxy.example.com:
    if (isInNet(host, "10.0.0.0", "255.255.248.0"))
    {
        return "PROXY fastproxy.example.com:8080";
    }

    // All other requests go through port 8080 of proxy.example.com.
```

```
// should that fail to respond, go directly to the WWW:  
return "PROXY proxy.example.com:8080; DIRECT";
```

Vorauthentifizierungs-ACL erstellen

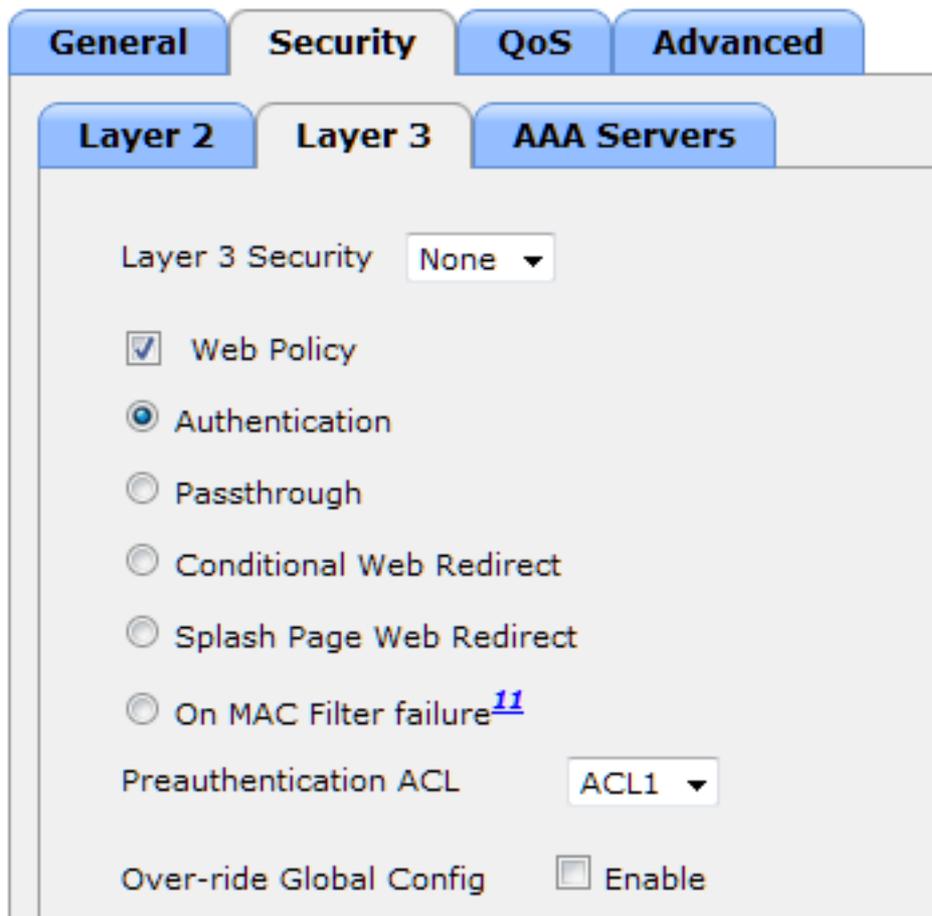
Platzieren Sie eine ACL für die Vorauthentifizierung auf der Web Authentication Service Set Identifier (SSID), sodass Wireless-Clients die PAC-Datei herunterladen können, bevor sich die Clients bei Web Auth anmelden. Die Zugriffskontrollliste für die Vorauthentifizierung muss nur den Port zulassen, an dem die PAC-Datei angeschlossen ist. Der Zugriff auf den Proxy-Port ermöglicht Clients, ohne Web-Authentifizierung auf das Internet zuzugreifen.

1. Navigieren Sie zu **Sicherheit > Zugriffskontrollliste**, um eine ACL für den Controller zu erstellen.
2. Erstellen Sie Regeln, um den Datenverkehr auf dem PAC-Download-Port für den Proxy in beide Richtungen zuzulassen.

| General | | | | | | | | | | |
|------------------|--------|-------------------|---------------------|----------|-------------|-----------|------|-----------|----------------|---|
| Access List Name | | ACL1 | | | | | | | | |
| Deny Counters | | 0 | | | | | | | | |
| Seq | Action | Source IP/Mask | Destination IP/Mask | Protocol | Source Port | Dest Port | DSCP | Direction | Number of Hits | |
| 1 | Permit | 0.0.0.0 / | 192.168.0.4 / | TCP | Any | 8081 | Any | Any | 0 |  |
| | | 0.0.0.0 / | 255.255.255.255 / | | | | | | | |
| 2 | Permit | 192.168.0.4 / | 0.0.0.0 / | TCP | 8081 | Any | Any | Any | 0 |  |
| | | 255.255.255.255 / | 0.0.0.0 / | | | | | | | |

Hinweis: Lassen Sie den Proxy-HTTP-Port nicht zu.

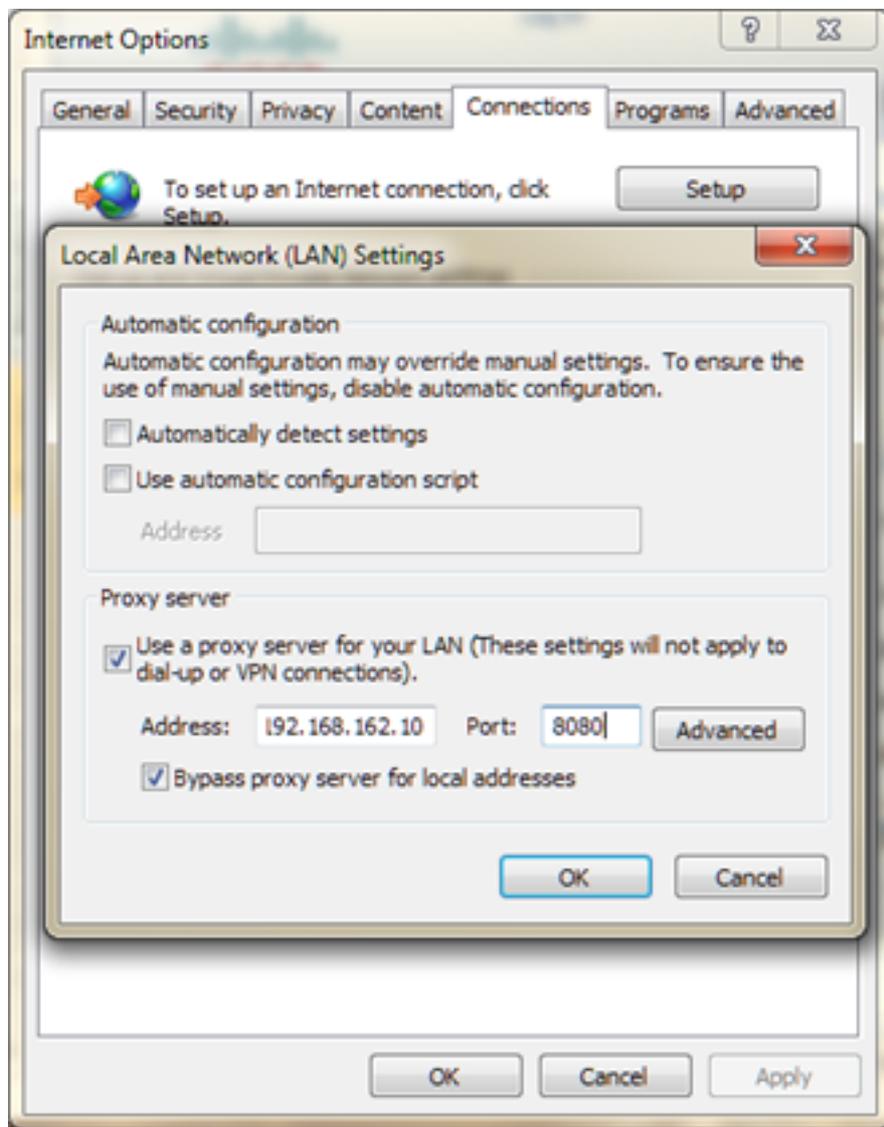
3. Vergessen Sie nicht, in der WLAN-Konfiguration des Controllers die ACL auszuwählen, die Sie gerade als Preauthentication-ACL erstellt haben.



Schnellreparatur: Webbrowser konfigurieren

In diesem Verfahren wird beschrieben, wie eine Ausnahme manuell konfiguriert wird, sodass ein Webbrowser des Clients direkt auf 192.0.2.1 ausreicht.

1. Navigieren Sie in Internet Explorer zu **Extras > Internetoptionen**.
2. Klicken Sie auf die Registerkarte **Verbindungen** und anschließend auf die Schaltfläche **LAN-Einstellungen**.
3. Aktivieren Sie im Proxy-Serverbereich das Kontrollkästchen **Proxyserver für LAN verwenden**, und geben Sie die IP-Adresse und den Port ein, an dem der Server lauscht.



4. Klicken Sie auf **Erweitert**, und geben Sie im Bereich Ausnahmen die virtuelle IP-Adresse des WLC ein.

Servers

| Type | Proxy address to use | Port |
|---------|---|----------------------|
| HTTP: | <input type="text" value="192.168.162.10"/> | <input type="text"/> |
| Secure: | <input type="text"/> | <input type="text"/> |
| FTP: | <input type="text"/> | <input type="text"/> |
| Socks: | <input type="text"/> | <input type="text"/> |

Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

Use semicolons (;) to separate entries.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.