Configuratievoorbeeld van webverificatie

Inhoud

Inleiding

Dit document beschrijft hoe u web verificatie kunt configureren om met een proxy-instelling te werken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basisconfiguratie van draadloze LAN-controllers
- Beveiliging van webverificatie

Gebruikte componenten

De informatie in dit document is gebaseerd op een Cisco draadloze LAN-controller, versie 7.0 en hoger.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Netwerkbeheerders die een proxy-server op hun netwerk hebben, verzenden eerst webverkeer naar de proxy-server, waarna het verkeer naar het internet wordt teruggebracht. De verbindingen tussen de client en de volmachtserver kunnen een TCP poort anders dan haven 80 voor

communicatie gebruiken. Deze poort is gewoonlijk TCP poort 3128 of 8080. Standaard luistert webverificatie alleen naar poort 80. Wanneer een HTTP GET de computer verlaat, wordt deze naar de proxy poort gestuurd maar door de controller laten vallen.

In deze sectie wordt beschreven hoe u web authenticatie kunt configureren om met een proxy installatie te werken:

1. Configureer de Cisco draadloze LAN-controller (WLC) om op de proxy-poort te luisteren.
2. Configureer het PAC-bestand (proxy-auto-configuratie) om het virtuele IP-adres direct op te geven.
3. Maak een toegangscontrolelijst voor verificatie (ACL) zodat de client het PAC-bestand kan downloaden voor web-verificatie.

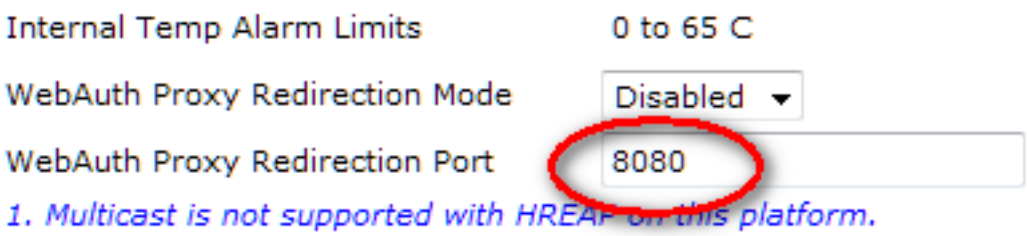
Als een snelle oplossing kunt u de browser handmatig configureren om 192.0.2.1 terug te geven.

Nadere details over elk van deze processen zijn te vinden in de volgende subsecties.

De WLC configureren

In deze procedure wordt beschreven hoe de poort wordt gewijzigd en hoe de controller luistert naar de poort waarop de proxy-server luistert.

1. Navigeer naar de **controller** > **General** pagina.

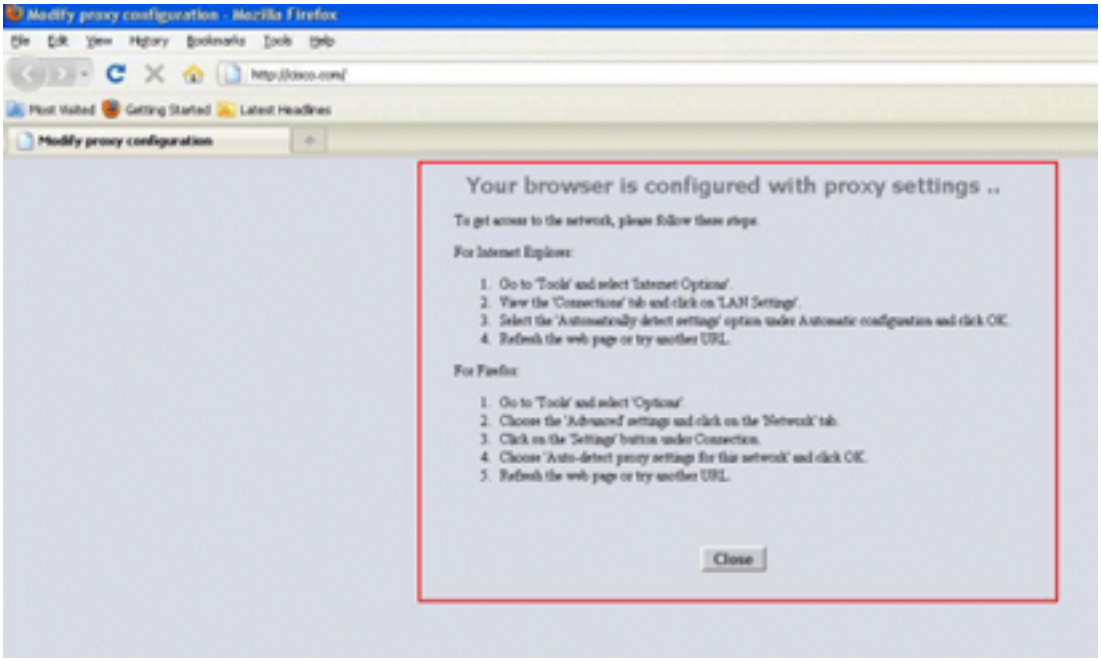


2. In het veld Webex Proxy omleiding geeft u de poort in die u wilt dat de WLC luistert naar client-omleiding.

3. Kies Uitgeschakeld of in de vervolgkeuzelijst Webex Proxy omleiding modus:

   Als u voor **Gehandicapten** kiest, worden de klanten de normale web authenticatie pagina voor passthrough of authenticatie voorgesteld. Dus als u een proxy gebruikt, moet u alle client browsers configureren om de proxy voor 192.0.2.1 niet te gebruiken (of een ander virtueel IP-adres dat het WLC gebruikt). Zie Web browser configureren.

   Als u **Ingeschakeld** kiest, luistert de WLC naar de poorten 80, 8080 en 3128 standaard. U hoeft deze poorten niet in het veld Webex Proxy omleiding poorttekst in te voeren. Als een client een HTTP GET op deze poorten stuurt, zien ze een scherm dat hen vraagt om hun proxy-instellingen automatisch te wijzigen.



4. Bewaar de configuratie.

5. Herstart de controller.

Geef in het kort een poortnummer op in de Webex Proxy-omleidingspoort om de poort te definiëren waarop de WLC-toets wordt gevolgd. Als de omleidingsmodus is ingeschakeld, stuurt deze de client terug naar het proxy-instellingsscherm en verwacht dynamisch een Web Proxy Auto-Discovery (WPAD) of PAC-bestand voor automatische proxy-configuratie te drukken. Indien uitgeschakeld, wordt de client omgeleid naar de normale web authenticatie pagina.

Het PAC-bestand configureren

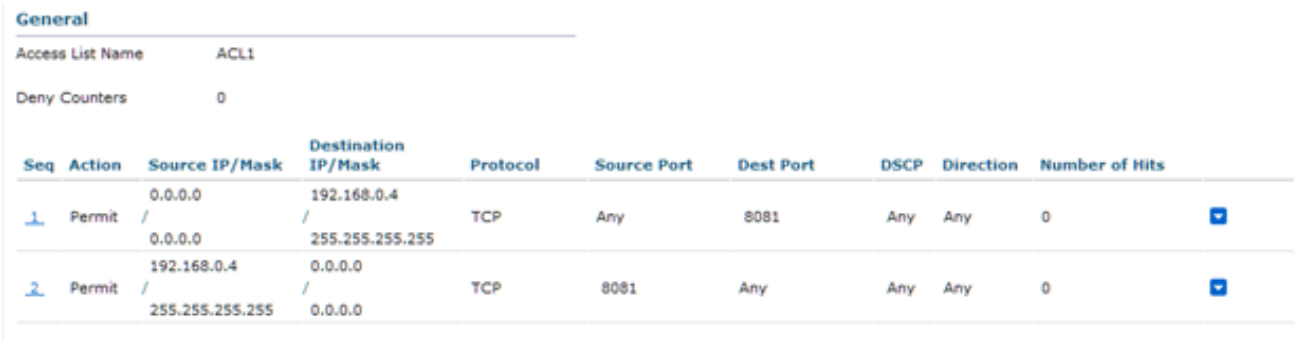
Het virtuele IP-adres van de WLC moet 'direct' worden teruggestuurd zodat de Web Auth gebruikers correct kan authenticeren. Direct betekent dat de proxy server het verzoek niet aanwijst, en de client heeft rechten om rechtstreeks het IP-adres te bereiken. Dit wordt gewoonlijk op de proxy server in het WPAD of PAC bestand ingesteld door de beheerder van de proxy server. Dit is een voorbeeldconfiguratie voor een PAC-bestand:

```
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";
```

Verificatie vooraf maken

Plaats een preauthenticatie ACL op de reeks ID (Web Verification Service) zodat draadloze klanten het PAC-bestand kunnen downloaden voordat de klanten in Web Auth loggen. De preauthenticatie ACL moet alleen toegang tot de poort van het PAC-bestand toestaan. Toegang tot de proxy poort maakt het mogelijk dat klanten het internet bereiken zonder web authenticatie.

1. Navigeer naar **Security > Access Control List** om een ACL op de controller te maken.
2. Maak regels om het verkeer op de PAC downloadpoort naar de proxy in beide richtingen toe te staan.



General

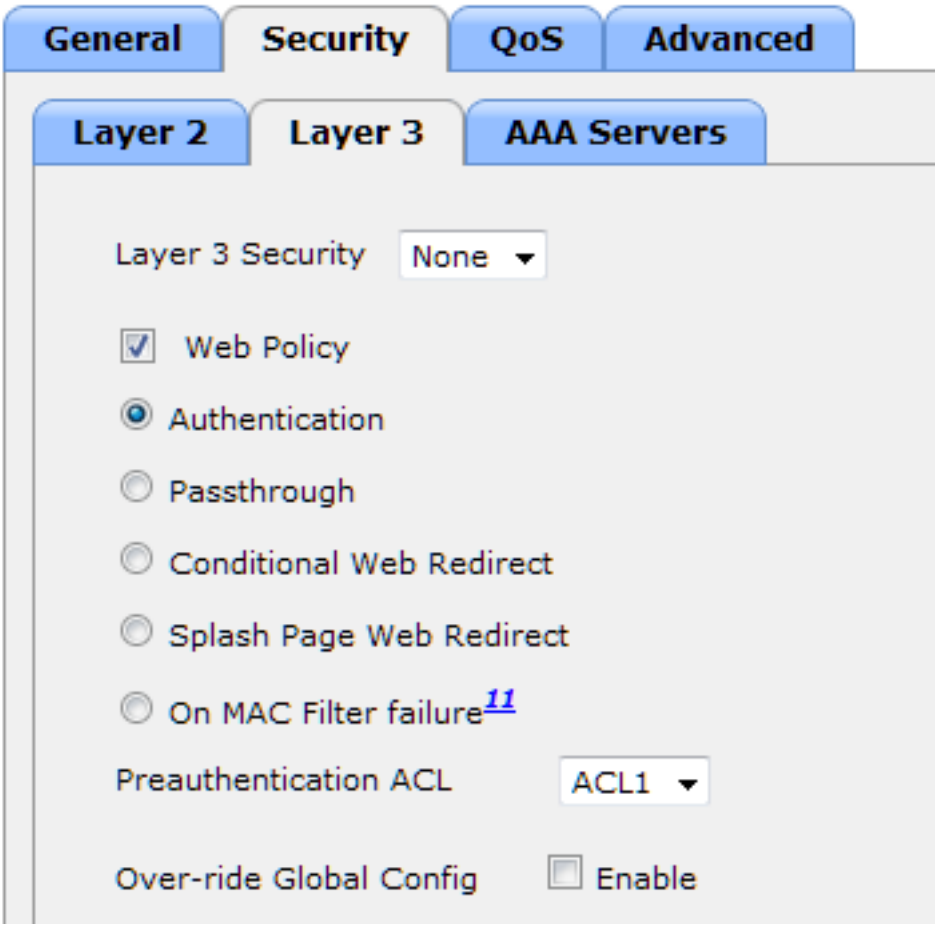
Access List Name ACL1

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 / 0.0.0.0	192.168.0.4 / 255.255.255.255	TCP	Any	8081	Any	Any	0
2	Permit	192.168.0.4 / 255.255.255.255	0.0.0.0 / 0.0.0.0	TCP	8081	Any	Any	Any	0

Opmerking:Laat de proxy-HTTP-poort niet toe.

3. In de WLAN-configuratie op de controller, vergeet niet de ACL te kiezen die u net hebt gemaakt als een voorverificatie.



Snel vastmaken: Web browser configureren

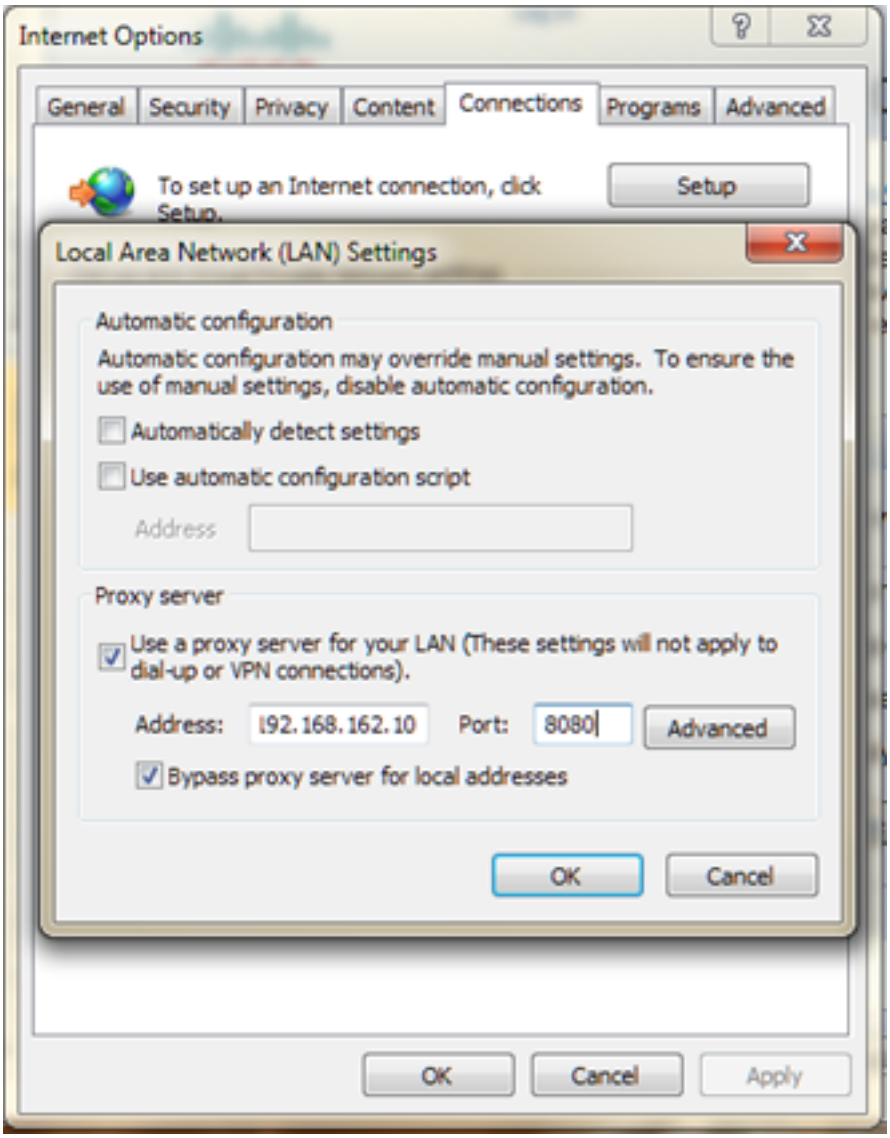
In deze procedure wordt beschreven hoe u een uitzondering handmatig kunt configureren, zodat

een browser van het client-web rechtstreeks tot 192.0.2.1 bereikt.

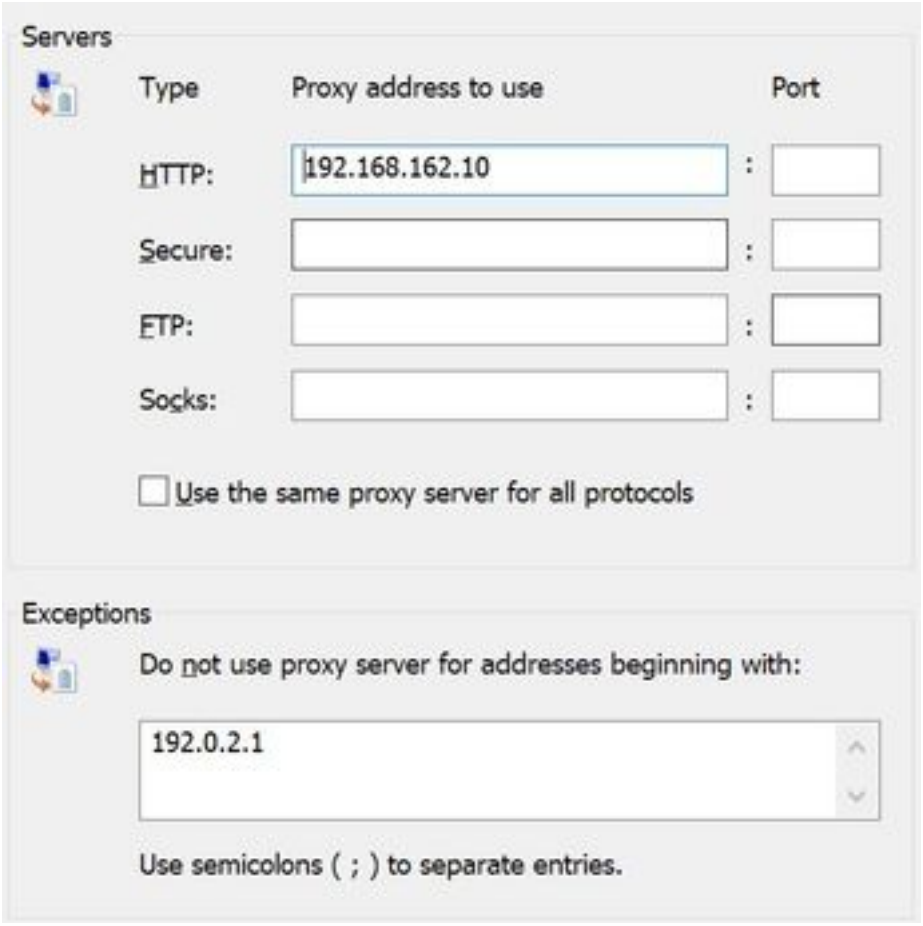
1. Navigeer in Internet Explorer naar **Gereedschappen** > **Internet-opties**.

2. Klik op het tabblad **Connections** en vervolgens op de knop **LAN-instellingen**.

3. In het gebied Proxyserver controleert u het vakje **Gebruik een proxy-server voor uw LAN** en voert u het (IP) Adres in en Port de server luistert.



4. Klik op **Geavanceerd** en voer het virtuele IP-adres van de WLC in het gebied Exceptions in.



Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.