Central-webverificatie met een Configuratievoorbeeld van Switch- en Identity Services Engine

Inhoud

Inleiding

Dit document beschrijft hoe u de centrale web authenticatie kunt configureren met bekabelde clients die zijn aangesloten op switches met behulp van Identity Services Engine (ISE).

Het concept van centrale web authenticatie is tegen lokale web authenticatie, wat de gebruikelijke web authenticatie op de switch zelf is. In dat systeem zal de switch, bij een storing van dot1x/mab, uitvallen op het webauteprofiel en het clientverkeer omleiden naar een webpagina van de switch.

Centrale web authenticatie biedt de mogelijkheid om een centraal apparaat te hebben dat fungeert als een webportaal (in dit geval de ISE). Het belangrijkste verschil in vergelijking met de gebruikelijke lokale web authenticatie is dat het wordt verschoven naar Layer 2 samen met mac/dot1x authenticatie. Het concept verschilt ook in die zin dat de Straalserver (ISE in dit voorbeeld) speciale eigenschappen teruggeeft die op de switch aangeven dat een webomleiding moet plaatsvinden. Deze oplossing heeft het voordeel dat iedere vertraging die nodig was om de web authenticatie te starten, wordt uitgebannen. Als het MAC-adres van het client-station niet bekend is door de Straalserver (maar er kunnen ook andere criteria worden gebruikt), geeft de server de redirectieeigenschappen terug en de schakelaar geeft toestemming voor het station (via

MAC-authenticatie bypass [MAB]) maar stelt een toegangslijst om het webverkeer naar het portal om te leiden. Zodra de gebruiker zich op het gastportaal inlogt, is het mogelijk via CoA (Veranderen van Vergunning) om de switchpoort te weerkaatsen zodat er een nieuwe Layer 2 MAB-verificatie plaatsvindt. ISE kan zich dan herinneren dat het een internetgebruiker was en Layer 2 eigenschappen (zoals dynamische VAN toewijzing) op de gebruiker toepast. Een ActiveX-component kan de client-PC ook dwingen om zijn IP-adres op te frissen.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Identity Services Engine (ISE)
- Cisco IOS®-switchconfiguratie

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Identity Services Engine (ISE), release 1.1.1
- Cisco Catalyst 3560 Series switch met softwareversie 12.2.55SE3

  Opmerking: De procedure is vergelijkbaar of identiek voor andere Catalyst switchmodellen. U kunt deze stappen op alle Cisco IOS-softwarereleases voor Catalyst gebruiken tenzij anders vermeld.

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

Overzicht

De configuratie van de ISE bestaat uit deze vijf stappen:

1. Maak de downloadbare toegangscontrolelijst (ACL).
2. Maak het vergunningprofiel.
3. Maak een authenticatieregel.
4. Maak een autorisatieregel.
5. Schakel de IP-vernieuwing in (optioneel).

Downloadbare ACL maken

Dit is geen verplichte stap. Hiermee wordt ACL-richting teruggestuurd naar het centrale webauth-profiel, dat bepaalt welk verkeer (HTTP of HTTPS) naar ISE wordt teruggeleid. Met deze ACL kunt

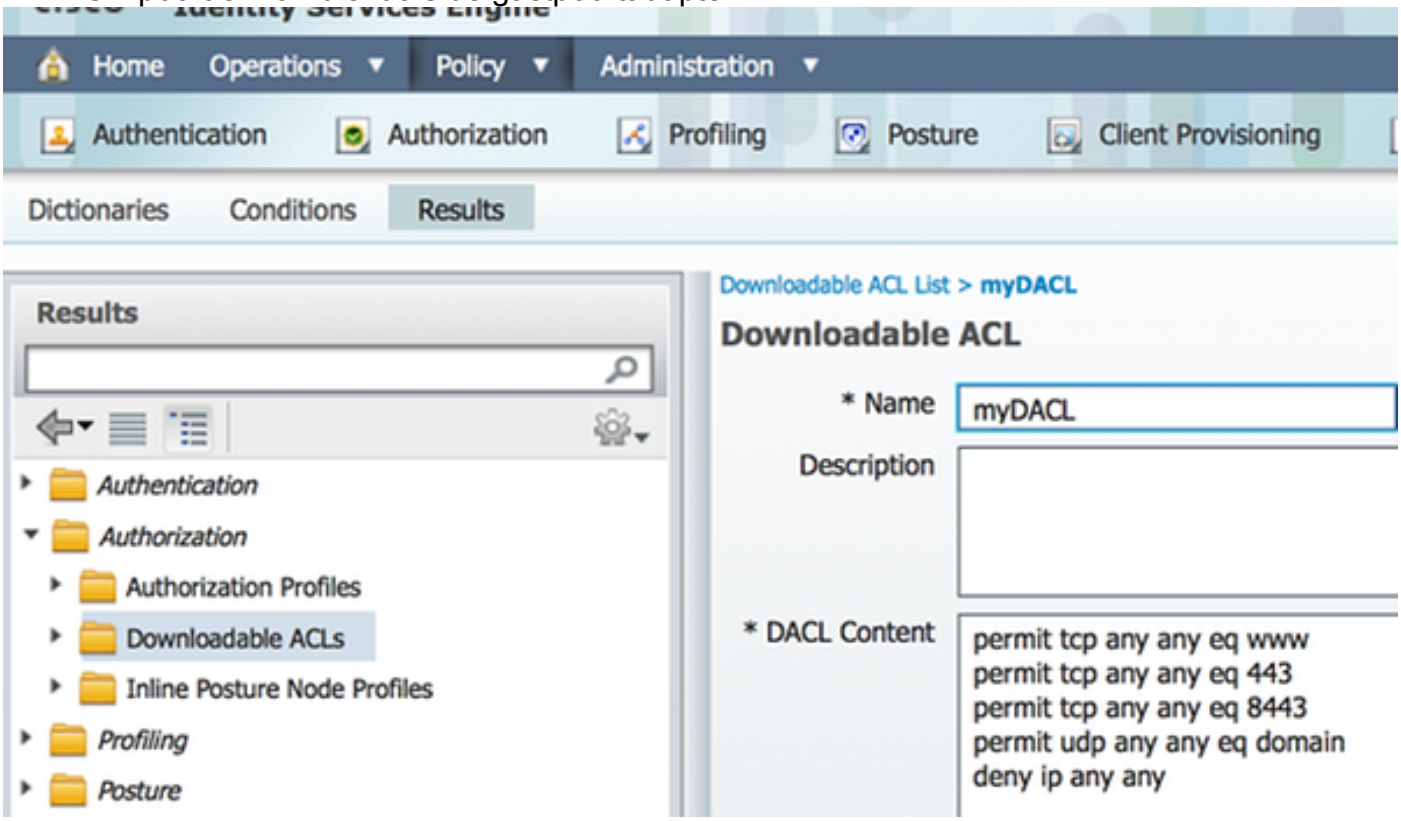
u definiëren wat het verkeer is toegestaan. U dient doorgaans DNS, HTTP(S) en 8443 mogelijk te maken en de rest te ontkennen. Anders richt de switch HTTP-verkeer op maar maakt hij andere protocollen mogelijk.

Voltooi deze stappen om het te downloaden ACL te maken:

1. Klik op **Beleid** en klik op **Elementen beleid**.
2. Klik op **Resultaten**.
3. Vergroot **de autorisatie** en klik op **Downloadbare ACL's**.
4. Klik op de knop **Toevoegen** om een nieuwe downloadbare ACL te maken.
5. Typ in het veld **Naam** een naam voor de DACL. Dit voorbeeld gebruikt *mijnDACL*.

Deze afbeelding toont een typische DACL-inhoud die:

- DNS - los de ISE-hostname op
- HTTP en HTTPS - toestaan van omleiding
- TCP-poort 8443 - dient als de gastpoortadapter



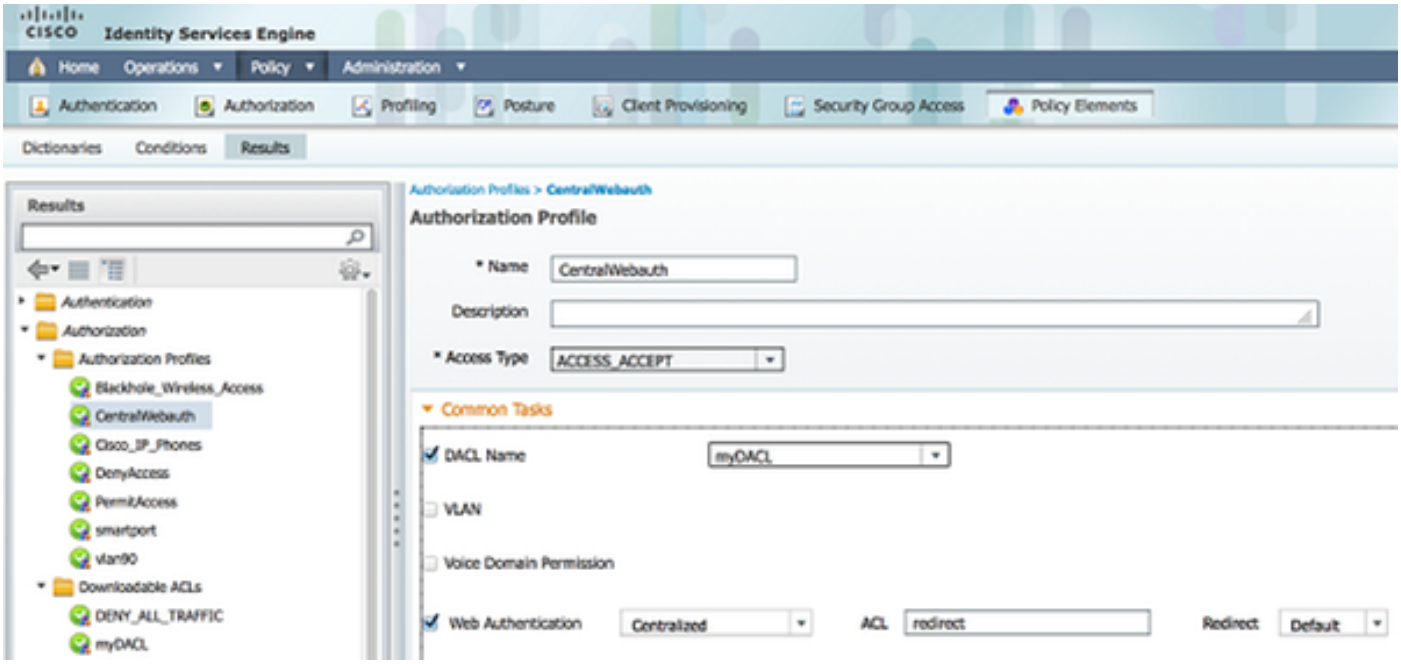
Maak het machtigingsprofiel

Voltooi deze stappen om het vergunningprofiel te creëren:

1. Klik op **Beleid** en klik op **Elementen beleid**.
2. Klik op **Resultaten**.
3. **Verbreek de autorisatie** en klik op **het autorisatieprofiel**.
4. Klik op de knop **Toevoegen** om een nieuw autorisatieprofiel voor een centrale website te maken.
5. Typ in het veld **Naam** een naam voor het profiel. Dit voorbeeld gebruikt *Central Webauth*.
6. Kies **ACCESS_ACCEPT** in de vervolgkeuzelijst Type toegang.
7. Controleer het vakje **Web Authentication** en kies **Centralized** in de vervolgkeuzelijst.

8. Voer in het veld ACL de naam van de ACL in op de schakelaar die het te herleiden verkeer definieert. Deze voorbeelden gebruiken *omleiding*.
9. Kies Standaard in de vervolgkeuzelijst Omzetten.
10. Controleer het selectieteken **van de Naam van** DACL, en kies **mijnDACL** van de vervolgkeuzelijst als u beslist een DACL in plaats van een statische poort op de schakelaar ACL te gebruiken.

De eigenschap Redirect definieert of ISE het standaard webportaal of een aangepast webportaal ziet dat door de ISE-beheerder gecreëerd is. Bijvoorbeeld, *om* ACL in dit voorbeeld *opnieuw te richten* veroorzaakt een omleiding op HTTP of HTTPS verkeer van de client naar overal. ACL wordt gedefinieerd op de schakelaar later in dit configuratievoorbeeld.

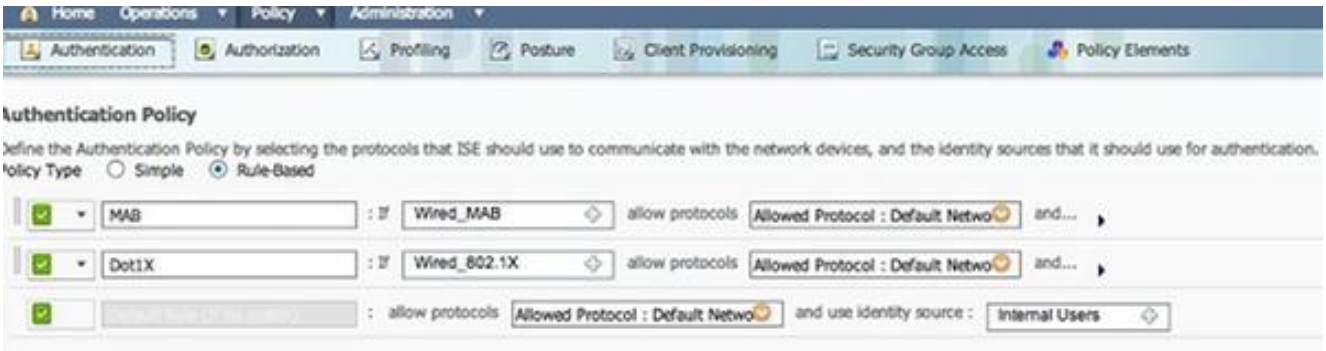


Een verificatieregel maken

Voltooi deze stappen om het authenticatieprofiel te gebruiken om de authenticatieregel te creëren:

1. Klik onder het menu Beleid op **Verificatie**.

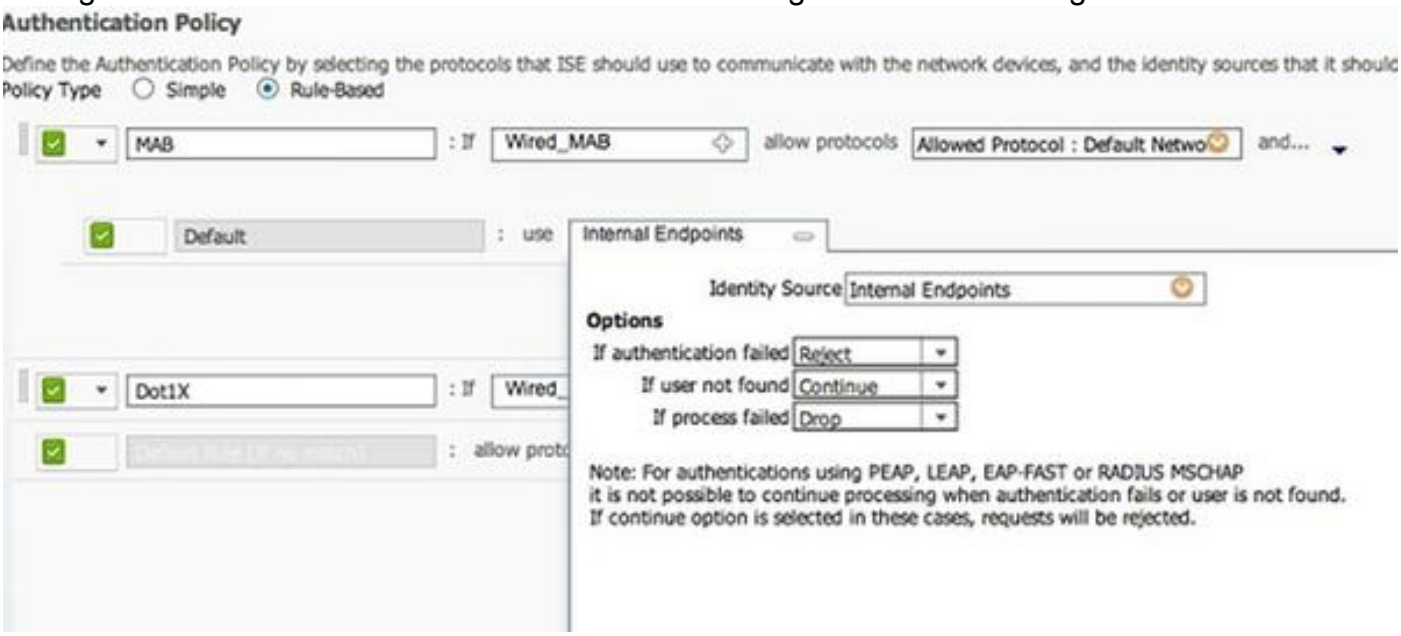
   Deze afbeelding toont een voorbeeld van hoe de regels van het authenticatiebeleid te configureren. In dit voorbeeld wordt een regel ingesteld die geactiveerd wanneer MAB wordt gedetecteerd.



2. Voer een naam in voor uw authenticatieregel. Dit voorbeeld gebruikt *MAB*.
3. Selecteer het pictogram plus (**+**) in het veld Indien u dit wilt doen.

4. Kies **samengestelde conditie** en kies **Wired_MAB**.
5. Klik op de pijl naast **en ...** om de regel verder uit te vouwen.
6. Klik op het pictogram **+** in het veld Identiteitsbron en kies **Interne endpoints**.
7. Kies **Doorgaan** vanuit de vervolgkeuzelijst 'Indien gebruiker niet gevonden'.

   Met deze optie kan een apparaat worden geauthentiseerd (via een website) zelfs als het MAC-adres niet bekend is. Dot1x klanten kunnen nog steeds authenticeren met hun geloofsbrieven en zouden zich niet met deze configuratie moeten bezighouden.



Maak een autorisatieregel

In het toelatingsbeleid moeten nu verschillende regels worden opgesteld. Wanneer de PC is aangesloten, gaat deze door MAB; aangenomen wordt dat het MAC-adres niet bekend is, dus worden de website en ACL teruggegeven. Deze *MAC onbekende* regel wordt in deze afbeelding weergegeven en is in deze sectie ingesteld:

Voltooi deze stappen om de vergunningsregel te creëren:

1. Maak een nieuwe regel, en voer een naam in. Dit voorbeeld gebruikt *MAC onbekend*.
2. Klik op het pictogram plus (**+**) in het veld Voorwaarde en kies om een nieuwe voorwaarde te maken.
3. Uitbreidt u de vervolgkeuzelijst **expressie**.
4. Kies **Netwerktoegang** en vergroot deze.
5. Klik op **Verificatiestatus** en kies de **equals** operator.
6. Kies **Onbekende gebruiker** in het veld Rechts.
7. Kies op de pagina Algemene toestemming **Central Webauth** (autorisatieprofiel) in het veld rechts van het woord *dan*.

   Deze stap laat ISE toe om door te gaan alhoewel de gebruiker (of de MAC) niet bekend is.

Onbekende gebruikers worden nu voorgesteld op de logpagina. Zodra zij hun geloofsbrieven hebben ingevoerd, worden zij echter opnieuw met een authentificatieverzoek op de ISE ingediend; daarom moet een andere regel worden ingesteld met een voorwaarde waaraan wordt voldaan indien de gebruiker een gastgebruiker is . In dit voorbeeld wordt *als UserIdentityGroup gelijk staat aan Guest* gebruikt, en wordt aangenomen dat alle gasten tot deze groep behoren.

8. Klik de handelsknop aan het eind van de *MAC niet bekende* regel aan, en kies om een nieuwe regel hierboven toe te voegen.

   Opmerking: Het is van groot belang dat deze nieuwe regel vóór de *onbekende* regel van de *MAC* komt.
9. Voer een naam in voor de nieuwe regel. Dit voorbeeld gebruikt *IS-a-GUEST*.
10. Kies een voorwaarde die aansluit bij uw gastgebruikers.

    Dit voorbeeld gebruikt *InterneGebruiker:IdentityGroup is gelijk aan Gast* omdat alle gastgebruikers zijn gebonden aan de *Gastgroep* (of een andere groep die u in uw sponsor instellingen hebt ingesteld).
11. Klik op **PermitAccess** in het resulterende vak (rechts van het woord *dan*).

    Wanneer de gebruiker op de Login-pagina is geautoriseerd, start ISE Layer 2-verificatie opnieuw op de switchpoort en verschijnt er een nieuwe MAB. In dit scenario is het verschil dat er een onzichtbare vlag is ingesteld voor ISE om te onthouden dat het een door gasten geauthentiseerde gebruiker was. Deze regel is *2de AUTH*, en de voorwaarde is *Network Access:UseCase Net GuestFlow.* Aan deze voorwaarde wordt voldaan wanneer de gebruiker via een website voor authentiek verklaart, en de switchpoort wordt opnieuw ingesteld voor een nieuwe MAB. U kunt elke eigenschap toewijzen die u wilt. Dit voorbeeld wijst een profiel *vlan90 toe* zodat de gebruiker VLAN 90 in zijn tweede MAB authenticatie wordt toegewezen.
12. Klik op **Handelingen** (gelegen aan het eind van de IS-a-GUEST regel) en kies **hierboven nieuwe regel invoegen**.
13. Voer **de tweede AUTH** in het veld Naam in.
14. In het veld conditionering klikt u op het **pictogram** plus (**+**) en vervolgens kiest u voor het maken van een nieuwe conditie.
15. Kies **netwerktoegang** en klik op **Case** gebruiken.
16. Kies **gelijken** als de operator.
17. Kies **GuestFlow** als de juiste operand.
18. Klik op de vergunningspagina op het pictogram plus (**+**) (naast *dan*) om een resultaat voor uw regel te kiezen.

    In dit voorbeeld wordt een vooraf ingesteld profiel (vlan90) toegewezen; deze configuratie wordt niet in dit document weergegeven.

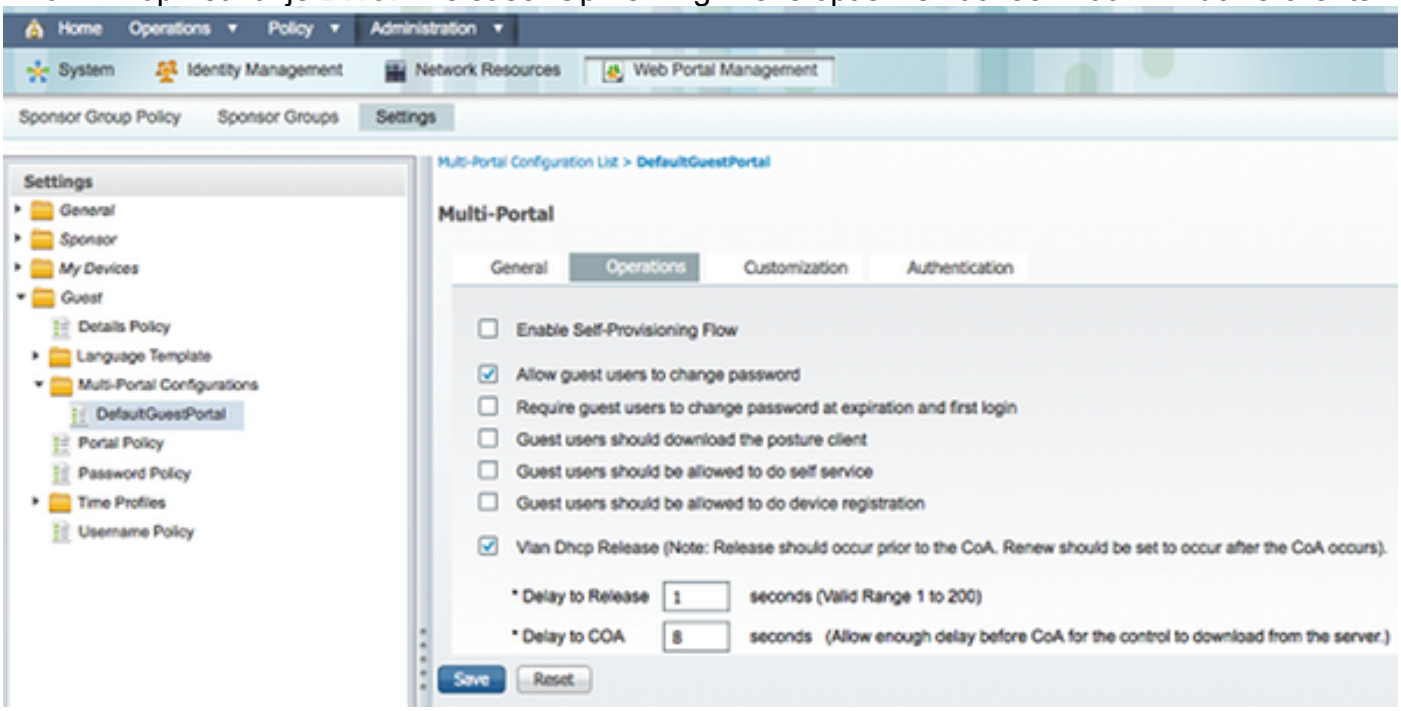
    U kunt een optie **Toegang toestaan** kiezen of een aangepast profiel maken om het VLAN of de eigenschappen die u leuk vindt terug te geven.

Schakel de IP-vernieuwing in (optioneel)

Als u een VLAN toewijst, is de laatste stap voor de client-PC om zijn IP-adres te vernieuwen. Deze stap wordt bereikt door het gastportaal voor Windows klanten. Als u geen VLAN voor de *tweede AUTH*-regel hebt ingesteld, kunt u deze stap overslaan.

Als u een VLAN hebt toegewezen, voltooi u deze stappen om IP-vernieuwing in te schakelen:

1. Klik op **Beheer** en klik op **Gastbeheer**.
2. Klik op **Instellingen**.
3. Uitbreidt **Guest** en breidt **de configuratie van meerdere portaalsites uit**.
4. Klik op **DefaultGuestPortal** of de naam van een aangepast portal dat u hebt gemaakt.
5. Klik op het vakje **DHCP** Release. Opmerking: Deze optie werkt alleen voor Windows-clients.



Switch-configuratie (fragment)

Dit gedeelte bevat een fragment van de switchconfiguratie. Zie Switch Configuration (Full) voor de volledige configuratie.

Deze steekproef toont een eenvoudige MAB configuratie.

```
interface GigabitEthernet1/0/12
description ISE1 - dot1x clients - UCS Eth0
switchport access vlan 100
switchport mode access
ip access-group webauth in
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
end
```

VLAN 1000 is het VLAN dat volledige netwerkconnectiviteit biedt. Een standaardpoort op ACL (genaamd *webauth*) wordt toegepast en gedefinieerd zoals hieronder wordt getoond:

```
ip access-list extended webauth
```

```
permit ip any any
```

Deze voorbeeldconfiguratie geeft volledige toegang tot het netwerk, zelfs indien de gebruiker niet echt is bevonden; daarom kunt u de toegang tot niet - geauthentiseerde gebruikers beperken .

In deze configuratie, werkt HTTP en HTTPS het bladeren niet zonder authenticatie (per andere ACL) omdat ISE is geconfigureerd om ACL (genaamd *omleiden*) te gebruiken. Hier is de definitie op de schakelaar:

```
ip access-list extended redirect
deny ip any host <ISE ip address>
permit TCP any any eq www
permit TCP any any eq 443
```

Deze toegangslijst moet op de schakelaar worden gedefinieerd om te bepalen op welk verkeer de schakelaar de omleiding zal uitvoeren. (Het komt overeen met een *vergunning*.) In dit voorbeeld, elk HTTP of HTTPS verkeer dat de client verstuurt, veroorzaakt een web redirectie. Dit voorbeeld ontkent ook het ISE IP adres zodat het verkeer naar ISE naar ISE gaat en niet in een lus opnieuw richt. (In dit scenario blokkeert ontkennen het verkeer niet; het omleiden van het verkeer is gewoon niet mogelijk .) Als u ongebruikelijke HTTP poorten of een proxy gebruikt, kunt u andere poorten toevoegen.

Een andere mogelijkheid is om HTTP toegang te verlenen tot bepaalde websites en andere websites te heroriënteren. Als u bijvoorbeeld in ACL een vergunning voor interne web servers definieert, kunnen klanten het web bladeren zonder authenticatie maar zouden ze de redirect tegenkomen als ze een interne webserver proberen te bereiken.

De laatste stap is om CoA op de schakelaar toe te staan. Anders kan ISE de schakelaar niet dwingen om de client opnieuw te authentiseren.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```

Deze opdracht is vereist voor de schakelaar om te richten op basis van HTTP-verkeer:

```
ip http server
```

Deze opdracht is vereist om opnieuw te sturen op basis van HTTPS-verkeer:

```
ip http secure-server
```

Deze opdrachten zijn ook belangrijk:

```
radius-server vsa send authentication
radius-server vsa send accounting
```

Als de gebruiker nog niet echt is bevonden, **geeft** de **show** op **authenticatie sessie in <interface num>** deze uitvoer terug:

```
01-SW3750-access#show auth sess int gi1/0/12
Interface: GigabitEthernet1/0/12
MAC Address:  000f.b049.5c4b
          IP Address:  192.168.33.201
           User-Name:  00-0F-B0-49-5C-4B
              Status:  Authz Success
```

```
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  N/A
             ACS ACL:  xACSACLx-IP-myDACL-51519b43
    URL Redirect ACL:  redirect
        URL Redirect:  https://ISE2.wlaaan.com:8443/guestportal/gateway?
sessionId=C0A82102000002D8489E0E84&action=cwa
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A82102000002D8489E0E84
     Acct Session ID:  0x000002FA
              Handle:  0xF60002D9

Runnable methods list:

      Method   State
      mab      Authc Success
```

Opmerking: Ondanks een succesvolle MAB-verificatie wordt de herdirect ACL geplaatst aangezien het MAC-adres niet bekend was bij ISE.

Switch-configuratie (volledig)

Deze sectie toont de volledige switchconfiguratie. Sommige overbodige interfaces en opdrachtlijnen zijn weggelaten; deze steekproefsamenstelling dient derhalve uitsluitend ter referentie te worden gebruikt en dient niet te worden gekopieerd .

```
Building configuration...

Current configuration : 6885 bytes
!
version 15.0
no service pad
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
no service password-encryption
!
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$xqtx$VPsZHbpGmLyH/EOObPpla.
!
aaa new-model
!
!
aaa group server radius newGroup
!
aaa authentication login default local
aaa authentication dot1x default group radius
aaa authorization exec default none
aaa authorization network default group radius
!
!
!
!
```

```
aaa server radius dynamic-author
client 192.168.131.1 server-key cisco
!
aaa session-id common
clock timezone CET 2 0
system mtu routing 1500
vtp interface Vlan61
udld enable

nmsp enable
ip routing
ip dhcp binding cleanup interval 600
!
!
ip dhcp snooping
ip device tracking
!
!
crypto pki trustpoint TP-self-signed-1351605760
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-1351605760
revocation-check none
rsakeypair TP-self-signed-1351605760
!
!
crypto pki certificate chain TP-self-signed-1351605760
certificate self-signed 01
30820245 308201AE A0030201 02020101 300D0609 2A864886 F70D0101 04050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274
69666963 6174652D 31333531 36303537 3630301E 170D3933 30333031 30303033
35385A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D31 33353136
30353736 3030819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100B068 86D31732 E73D2FAD 05795D6D 402CE60A B93D4A88 C98C3F54 0982911D
D211EC23 77734A5B 7D7E5684 388AD095 67354C95 92FD05E3 F3385391 8AB9A866
B5925E04 A846F740 1C9AC0D9 6C829511 D9C5308F 13C4EA86 AF96A94E CD57B565
92317B2E 75D6AB18 04AC7E14 3923D3AC 0F19BC6A 816E6FA4 5F08CDA5 B95D334F
DA410203 010001A3 6D306B30 0F060355 1D130101 FF040530 030101FF 30180603
551D1104 11300F82 0D69696C 796E6173 2D333536 302E301F 0603551D 23041830
16801457 D1216AF3 F0841465 3DDDD4C9 D08E06C5 9890D530 1D060355 1D0E0416
041457D1 216AF3F0 8414653D DDD4C9D0 8E06C598 90D5300D 06092A86 4886F70D
01010405 00038181 0014DC5C 2D19D7E9 CB3E8ECE F7CF2185 32D8FE70 405CAA03

dot1x system-auth-control
dot1x critical eapol
!
!
!
errdisable recovery cause bpduguard
errdisable recovery interval 60
!
spanning-tree mode pvst
spanning-tree logging
spanning-tree portfast bpduguard default
spanning-tree extend system-id
spanning-tree vlan 1-200 priority 24576
!
vlan internal allocation policy ascending
lldp run
!
!
!
!
!
```

```
!
interface FastEthernet0/2
switchport access vlan 33
switchport mode access
authentication order mab
authentication priority mab
authentication port-control auto
mab
spanning-tree portfast
!
interface Vlan33
ip address 192.168.33.2 255.255.255.0
!
ip default-gateway 192.168.33.1
ip http server
ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 192.168.33.1
!
ip access-list extended MY_TEST
permit ip any any
ip access-list extended redirect
deny ip any host 192.168.131.1
permit tcp any any eq www
permit tcp any any eq 443
ip access-list extended webAuthList
permit ip any any
!
ip sla enable reaction-alerts
logging esm config
logging trap warnings
logging facility auth
logging 10.48.76.31
snmp-server community c3560public RO
snmp-server community c3560private RW
snmp-server community private RO
radius-server host 192.168.131.1 auth-port 1812 acct-port 1813 key cisco
radius-server vsa send authentication
radius-server vsa send accounting
!
!
!
privilege exec level 15 configure terminal
privilege exec level 15 configure
privilege exec level 2 debug radius
privilege exec level 2 debug aaa
privilege exec level 2 debug
!
line con 0
line vty 0 4
exec-timeout 0 0
password Cisco123
authorization commands 1 MyTacacs
authorization commands 2 MyTacacs
authorization commands 15 MyTacacs
authorization exec MyTacacs
login authentication MyTacacs
line vty 5 15
!
ntp server 10.48.76.33
end
```

HTTP-proxyconfiguratie

Als je een HTTP proxy voor je klanten gebruikt, betekent dat dat je klanten:

- Gebruik een onconventionele poort voor HTTP-protocol
- Stuur al hun verkeer naar die proxy

Gebruik deze opdrachten om de schakelaar op de onconventionele poort te laten luisteren (bijvoorbeeld 8080):

```
ip http port 8080
ip port-map http port 8080
```

U moet ook alle klanten configureren om hun proxy te blijven gebruiken maar de proxy voor het ISE IP-adres niet te gebruiken. Alle browsers bevatten een eigenschap die u toestaat om gastnamen of IP adressen in te gaan die de volmacht niet zouden moeten gebruiken. Als u de uitzondering voor de ISE niet toevoegt, wordt er een pagina voor de herhalingsverificatie weergegeven.

U moet ook uw omleiding ACL wijzigen om op de volmachtpoort (8080 in dit voorbeeld) toe te staan.

Belangrijke opmerking over switch-SVI's

Op dit moment heeft de switch een virtuele interface (SVI) tussen verschillende interfaces nodig om naar de client te kunnen reageren en de portaalomleiding naar de client te kunnen doorsturen. Deze SVI hoeft niet noodzakelijkerwijs op de clientsubbus/VLAN te zijn. Als de switch echter geen SVI in clientsubtype/VLAN heeft, moet hij een van de andere SVI's gebruiken en verkeer verzenden zoals gedefinieerd in de client-routingtabel. Dit betekent doorgaans het verkeer naar een andere poort in de kern van het netwerk; dit verkeer komt terug naar de toegangsschakelaar binnen clientnet.

Firewalls blokkeren doorgaans het verkeer van en naar dezelfde switch, zoals in dit scenario, zodat een omleiding mogelijk niet goed werkt. De zorgpunten zijn om dit gedrag op de firewall toe te staan of om een SVI op de toegangsschakelaar in clientsubnet te creëren.

Belangrijke opmerking over HTTPS-omleiding

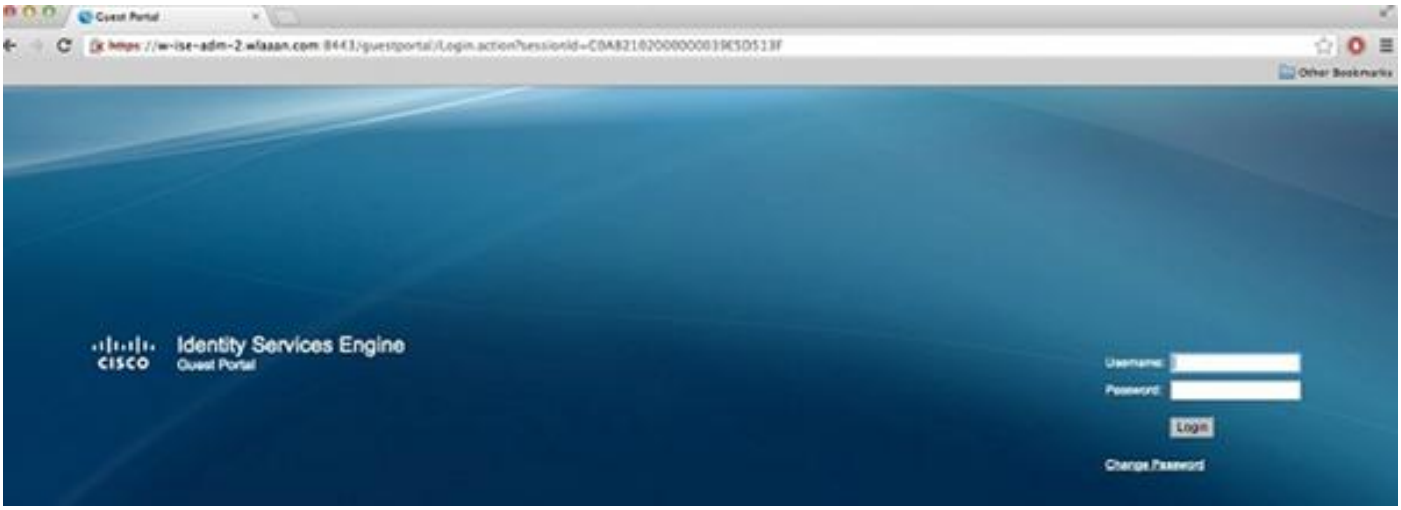
Switches kunnen HTTPS-verkeer omleiden. Dus als de gast cliënt een homepage in HTTPS heeft, gebeurt de omleiding correct.

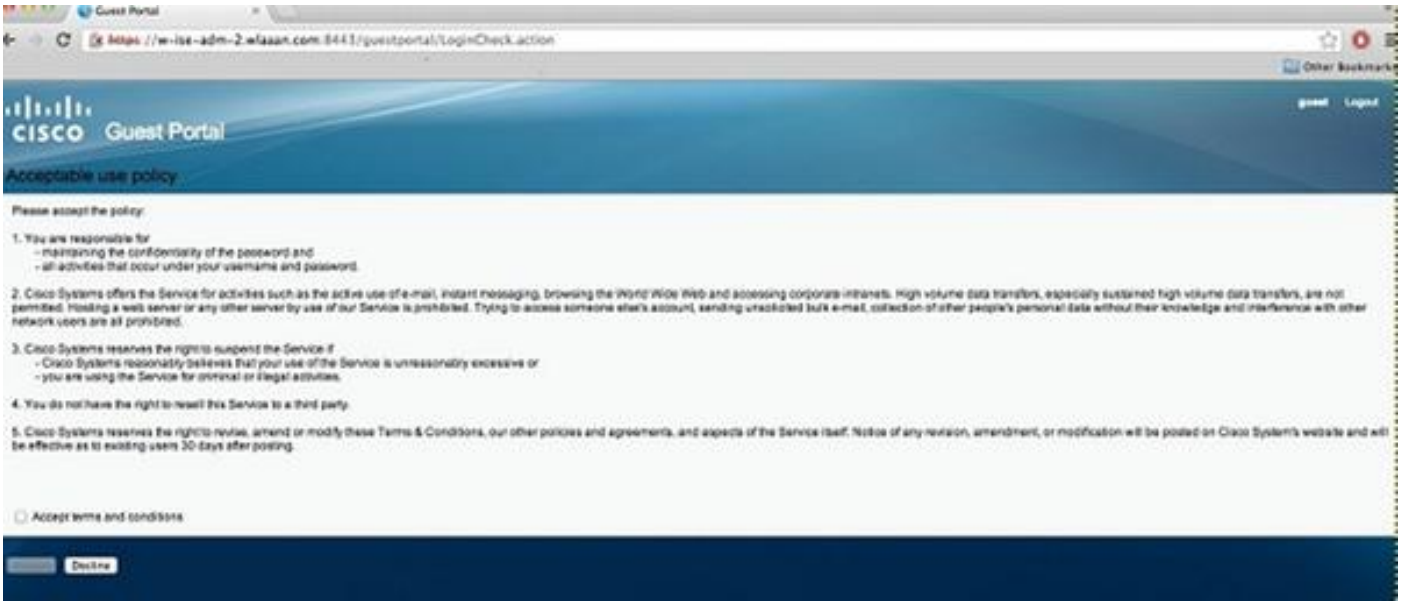
Het hele concept van omleiding is gebaseerd op het feit dat een apparaat (in dit geval de switch) het IP-adres van de website beslaat. Er doet zich echter een belangrijk probleem voor wanneer de schakelaar HTTPS-verkeer onderschept en omwijst omdat de switch alleen zijn eigen certificaat kan presenteren in de TLS-handdruk (Transport Layer Security). Omdat dit niet het certificaat is dat de oorspronkelijk gevraagde website is, geven de meeste webbrowsers belangrijke waarschuwingen uit. De browsers behandelen correct de omleiding en presentatie van een ander certificaat als veiligheidszorg. Hier is geen tijdelijke oplossing voor en de overstap naar parodie op het oorspronkelijke websitecertificaat is niet mogelijk.

Eindresultaat

De client-PC steekt in en voert MAB uit. Het adres van MAC is niet bekend, dus ISE duwt de omleidingseigenschappen terug naar de schakelaar. De gebruiker probeert een website te

raadplegen en wordt opnieuw gericht.





Wanneer de authenticatie van de loginpagina succesvol is, start ISE de omschakeling door Verandering van Vergunning, die opnieuw een Layer 2 MAB authenticatie begint.

ISE weet echter dat het een voormalige webauth client is en autoriseert de client op basis van de internetgeloofsbrieven (hoewel dit een Layer 2-authenticatie is).

In de ISE-authenticatiebestanden verschijnt de MAB-authenticatie onderaan het log. Hoewel het onbekend is, werd het MAC-adres geauthentiseerd en geprofileerd, en werden de webauteigenschappen teruggegeven. Daarna komt verificatie voor met de gebruikersnaam (dat wil zeggen, de gebruikerstypen zijn aanmeldingspagina). Onmiddellijk na verificatie treedt een nieuwe Layer 2-verificatie op met de gebruikersnaam als geloofsbrieven; deze authenticatiestap is waar u eigenschappen zoals dynamisch VLAN kunt teruggeven.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

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

Gerelateerde informatie

- Cisco Identity Services Engine
- Referentie voor Cisco Identity Services Engine
- Integratie met ISE (Identity Services Engine) met Cisco WLC (draadloze LAN-controller)
- Verzoeken om opmerkingen (RFC's)
- Technische ondersteuning en documentatie – Cisco Systems