스위치 및 ISE(Identity Services Engine)를 사용한 중앙 웹 인증 구성 예

목차

소개

이 문서에서는 ISE(Identity Services Engine)의 도움을 받아 스위치에 연결된 유선 클라이언트를 사용하여 중앙 웹 인증을 구성하는 방법에 대해 설명합니다.

중앙 웹 인증 개념은 스위치 자체에서 일반적인 웹 인증인 로컬 웹 인증과 반대됩니다.이 시스템에서 dot1x/mab 실패 시 스위치는 webauth 프로필로 장애 조치되고 클라이언트 트래픽을 스위치의 웹 페이지로 리디렉션합니다.

중앙 웹 인증은 웹 포털(예: ISE)의 역할을 하는 중앙 디바이스를 가질 수 있습니다. 일반적인 로컬 웹 인증과 비교했을 때 큰 차이점은 mac/dot1x 인증과 함께 레이어 2로 이동된다는 것입니다.이 예제의 ISE(radius 서버)는 웹 리디렉션이 발생해야 함을 스위치에 나타내는 특수 특성을 반환한다는 개념도 다릅니다.이 솔루션은 웹 인증에 필요한 지연을 제거할 수 있는 장점이 있습니다.전역적으로, 클라이언트 스테이션의 MAC 주소가 radius 서버에서 알지 못하는 경우(그러나 다른 기준도 사용할 수 있음), 서버는 리디렉션 특성을 반환하며, 스위치는 MAB(MAC 인증 우회)를 통해 스테이션에 권한을 부여하지만 웹 트래픽을 포털로 리디렉션하기 위한 액세스 목록을 배치합니다.사용자가 게스트 포털에 로그인하면 CoA(Change of Authorization)를 통해 스위치 포트를 바운스하여 새 레이어 2 MAB 인증이 발생할 수 있습니다.그런 다음 ISE는 webauth 사용자였다는 것을 기억할 수 있으며 사용자에게 레이어 2 특성(동적 VAN 할당 등)을 적용할 수 있습니다.ActiveX 구성 요소는 클라이언트 PC가 IP 주소를 새로 고침하도록 강제할 수도 있습니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- ISE(Identity Services Engine)
- Cisco IOS® 스위치 구성

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco ISE(Identity Services Engine), 릴리스 1.1.1
- 소프트웨어 버전 12.2.55SE3을 실행하는 Cisco Catalyst 3560 Series 스위치

  참고:이 절차는 다른 Catalyst 스위치 모델과 유사하거나 동일합니다.별도의 언급이 없는 한 모든 Cisco IOS Software Release for Catalyst에서 이 단계를 사용할 수 있습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

개요

ISE 컨피그레이션은 다음 5단계로 구성됩니다.

1. 다운로드 가능한 ACL(Access Control List)을 만듭니다.
2. 권한 부여 프로파일을 생성합니다.
3. 인증 규칙을 생성합니다.
4. 권한 부여 규칙을 생성합니다.
5. IP 갱신을 활성화합니다(선택 사항).

다운로드 가능한 ACL 생성

이는 필수 단계가 아닙니다.중앙 웹 인증 프로파일과 함께 다시 전송된 리디렉션 ACL은 어떤 트래픽(HTTP 또는 HTTPS)이 ISE로 리디렉션되는지를 결정합니다.다운로드 가능한 ACL을 사용하면 허용되는 트래픽을 정의할 수 있습니다.일반적으로 DNS, HTTP(S) 및 8443을 허용하고 나머지는 거부해야 합니다.그렇지 않으면 스위치는 HTTP 트래픽을 리디렉션하지만 다른 프로토콜을 허용합니다.

다운로드 가능한 ACL을 생성하려면 다음 단계를 완료합니다.

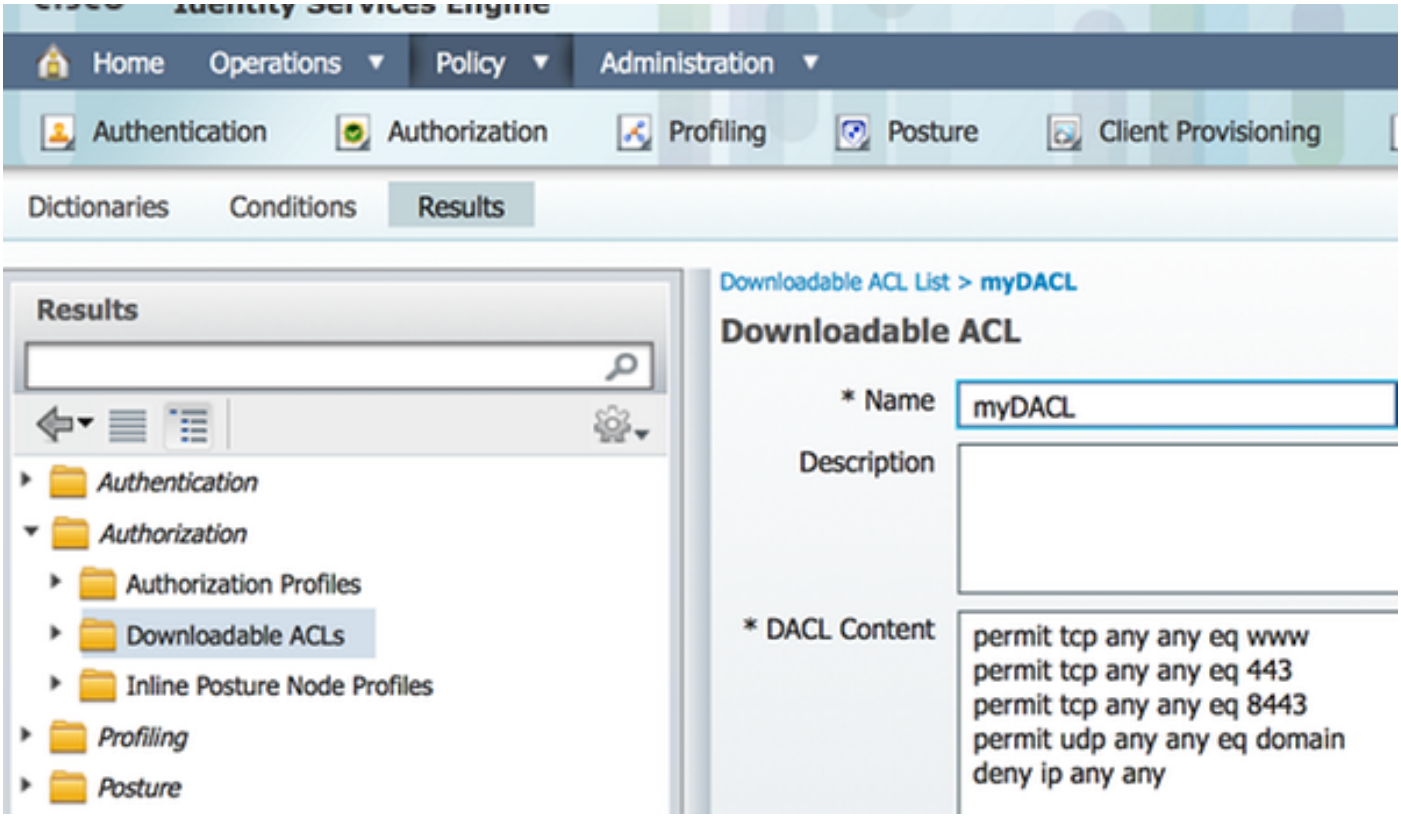
1. Policy(**정책**)를 클릭하고 **Policy Elements(정책 요소)를 클릭합니다**.
2. **결과**를 **클릭합니다**.
3. Authorization(권한 **부여**)을 확장하고 Downloadable ACLs(다운로드 가능한 **ACL)를 클릭합니**

다.

4. 다운로드 **가능한** 새 ACL을 생성하려면 Add(추가) 버튼을 클릭합니다.
5. Name(**이름**) 필드에 DACL의 이름을 입력합니다.이 예에서는 myDACL을 *사용합니다*.

이 그림에서는 다음과 같은 일반적인 DACL 내용을 보여 줍니다.

- DNS - ISE 포털 호스트 이름 확인
- HTTP 및 HTTPS - 리디렉션 허용
- TCP 포트 8443 - 게스트 포털 포트 역할



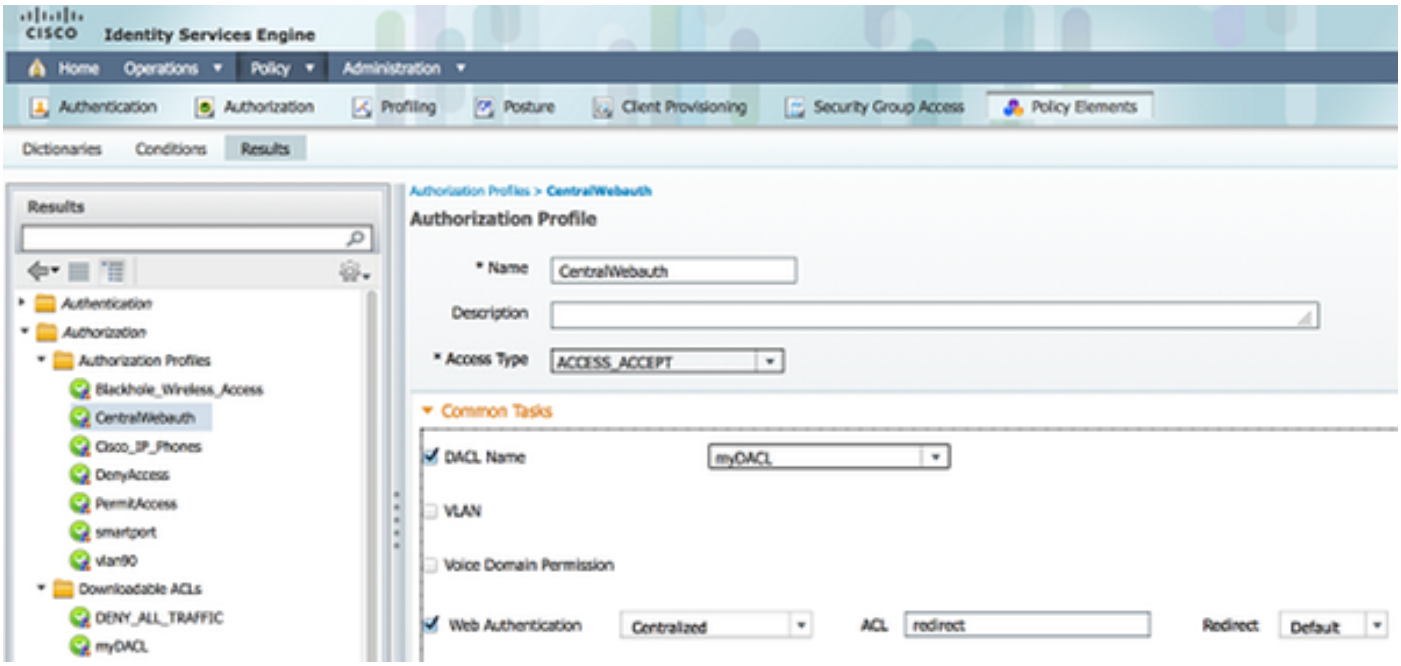
권한 부여 프로파일 생성

권한 부여 프로파일을 생성하려면 다음 단계를 완료합니다.

1. Policy(**정책**)를 클릭하고 **Policy Elements(정책 요소)를 클릭합니다**.
2. **결과**를 **클릭합니다**.
3. Authorization(권한 **부여**)을 확장하고 Authorization **profile(권한 부여 프로파일)**을 클릭합니다.
4. 중앙 WebUth에 대한 새 권한 부여 프로파일을 생성하려면 Add(**추가**) 버튼을 클릭합니다.
5. Name(**이름**) 필드에 프로파일 이름을 입력합니다.이 예제에서는 CentralWebauth를 *사용합니다*.
6. 액세스 **유형** 드롭다운 목록에서 ACCESS_ACCEPT를 선택합니다.
7. **Web Authentication(웹 인증**) 확인란을 선택하고 드롭다운 목록에서 Centralized(중앙 집중식)를 선택합니다.
8. ACL 필드에 리디렉션할 트래픽을 정의하는 스위치의 ACL 이름을 입력합니다.이 예에서는 *리디렉션*을 사용합니다.
9. Redirect 드롭다운 목록에서 Default를 선택합니다.
10. DACL **Name(DACL 이름**) 확인란을 선택하고 스위치**에서** 고정 포트 ACL 대신 DACL을 사용하려는 경우 드롭다운 목록에서 myDACL을 선택합니다.

Redirect 특성은 ISE에 기본 웹 포털 또는 ISE 관리자가 생성한 사용자 지정 웹 포털이 표시되는지 여부를 정의합니다.예를 들어 이 예에서 *리디렉션* ACL은 클라이언트에서 임의의 위치로 HTTP 또

는 HTTPS 트래픽에 대한 리디렉션을 트리거합니다.ACL은 이 컨피그레이션 예제의 뒷부분에서 스위치에 정의됩니다.

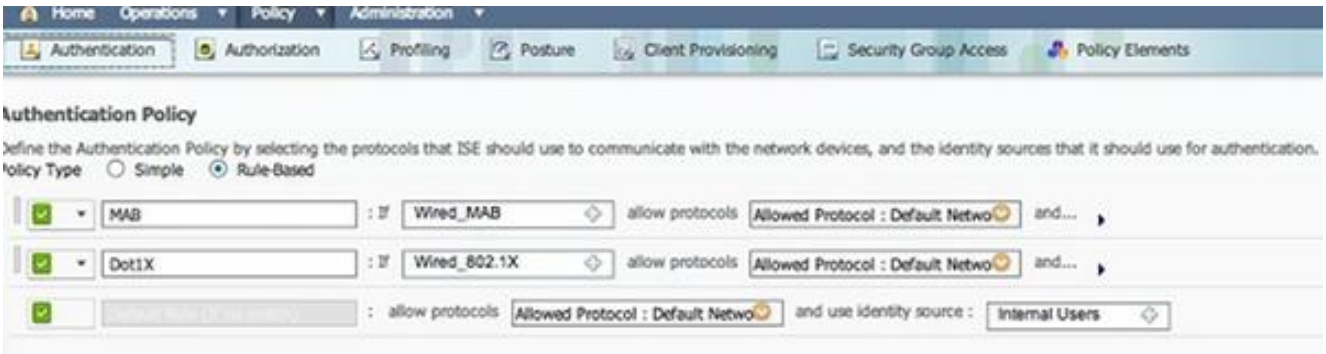


인증 규칙 생성

인증 프로필을 사용하여 인증 규칙을 생성하려면 다음 단계를 완료합니다.

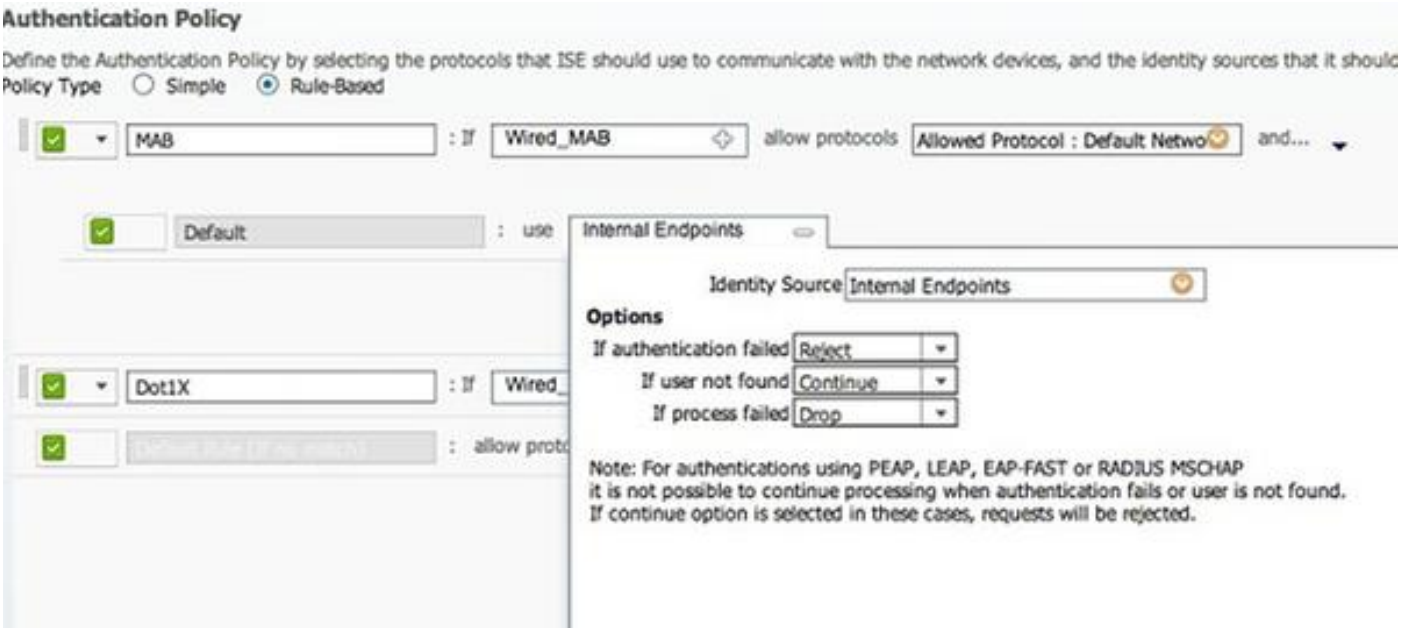
1. Policy(정책) 메뉴에서 Authentication(**인증**)을 클릭합니다.

   이 이미지는 인증 정책 규칙을 구성하는 방법의 예를 보여줍니다.이 예에서는 MAB가 탐지될 때 트리거되는 규칙이 구성됩니다.



2. 인증 규칙의 이름을 입력합니다.이 예에서는 MAB를 *사용합니다*.
3. If 조건 필드에서 더하기(**+**) 아이콘을 선택합니다.
4. Compound **condition(복합 조건)**을 선택하고 Wired_**MAB를 선택합니다**.
5. 규칙을 더 확장하려면 **및 ...** 옆에 있는 화살표를 클릭합니다.
6. Identity Source(ID 소스) 필드에서 **+** 아이콘을 클릭하고 Internal endpoints(내부 엔드포인트)를 **선택합니다**.
7. '사용자를 찾을 수 없는 경우' 드롭다운 목록에서 계속을 선택합니다.

   이 옵션을 사용하면 MAC 주소를 모르는 경우에도 디바이스를 인증할 수 있습니다(webauth를 통해).Dot1x 클라이언트는 여전히 해당 자격 증명으로 인증할 수 있으며 이 컨피그레이션에 대해 걱정하지 않아야 합니다.



권한 부여 규칙 생성

이제 권한 부여 정책에서 구성할 몇 가지 규칙이 있습니다.PC를 연결하면 MAB를 거칩니다.MAC 주소를 알 수 없으므로 webauth 및 ACL이 반환됩니다.이 *MAC* 규칙은 이 이미지에 표시되며 이 섹션에서 구성됩니다.

권한 부여 규칙을 생성하려면 다음 단계를 완료합니다.

1. 새 규칙을 생성하고 이름을 입력합니다.이 예에서는 *알 수 없는 MAC을* 사용합니다.
2. 조건 필드에서 더하기(**+**) 아이콘을 클릭하고 새 조건을 생성하도록 선택합니다.
3. 표현식 드롭다운 목록을 확장합니다.
4. Network **Access(네트워크 액세스)**를 선택하고 확장합니다.
5. AuthenticationStatus**를** 클릭하고 Equals **연산자를** 선택합니다.
6. 오른쪽 필드에서 UnknownUser를 선택합니다.
7. General Authorization(일반 권한 부여) 페이지의 단어 오른쪽 필드에서 CentralWebauth(Authorization Profile)를 *선택합니다*.

   이 단계에서는 사용자(또는 MAC)가 알려지지 않은 경우에도 ISE를 계속할 수 있습니다.

   알 수 없는 사용자가 로그인 페이지에 표시됩니다.그러나 자격 증명을 입력하면 ISE에 인증 요청이 다시 표시됩니다.따라서 사용자가 게스트 사용자일 경우 충족되는 조건으로 다른 규칙을 구성해야 합니다.이 예에서 UseridentityGroup이 *Guest와* 같은 경우 모든 게스트가 이 그룹에 속하는 것으로 간주됩니다.
8. *MAC*을 알 수 없는 규칙의 끝에 있는 작업 버튼을 클릭하고 위에 새 규칙을 삽입하도록 선택합니다.

   참고:이 새 규칙이 *MAC*에서 *알 수 없는* 규칙보다 우선한다는 것은 매우 중요합니다.
9. 새 규칙의 이름을 입력합니다.이 예에서는 *IS-a-GUEST를 사용합니다*.

10. 게스트 사용자와 일치하는 조건을 선택합니다.

    이 예에서는 모든 게스트 사용자가 *게스트* 그룹(또는 스폰서 설정에서 구성한 다른 그룹)에 바인딩되기 때문에 InternalUser:IdentityGroup Equals Guest를 사용합니다.
11. 결과 상자에서 허용(*다음* 단어 오른쪽에 있음) *액세스를* 선택합니다.

    사용자가 Login(로그인) 페이지에서 권한이 부여되면 ISE는 스위치 포트에서 레이어 2 인증을 다시 시작하고 새 MAB가 발생합니다.이 시나리오에서 차이점은 ISE가 게스트 인증 사용자임을 기억하도록 보이지 않는 플래그가 설정되었다는 것입니다.이 규칙은 *두 번째 AUTH*이며 조건은 Network Access:UseCase Equals *GuestFlow입니다*.사용자가 webauth를 통해 인증하고 새 MAB에 대해 스위치 포트가 다시 설정되면 이 조건이 충족됩니다.원하는 속성을 지정할 수 있습니다.이 예에서는 프로파일 vlan*90*을 할당하여 사용자가 두 번째 MAB 인증에서 VLAN 90을 할당합니다.
12. IS-a-GUEST 규칙의 끝에 있는 Actions(**작업**)를 클릭하고 **Insert new rule above(위에 새 규칙 삽입)를** 선택합니다.
13. 이름 필드**에 두 번째 AUTH**를 입력합니다.
14. 조건 필드에서 더하기(**+**) 아이콘을 클릭하고 새 조건을 생성하도록 선택합니다.
15. Network **Access(네트워크 액세스**)를 선택하고 UseCase를 **클릭합니다**.
16. 연산자로 Equals를 선택합니다.
17. GuestFlow**를** 오른쪽 피연산자로 선택합니다.
18. 규칙의 결과를 선택하려면 권한 부여 페이지에서 더하기(**+**) 아이콘(*그 다음* 옆에 있음)을 클릭합니다.

    이 예에서는 사전 구성된 프로파일(vlan90)이 할당됩니다.이 구성은 이 문서에 표시되지 않습니다.

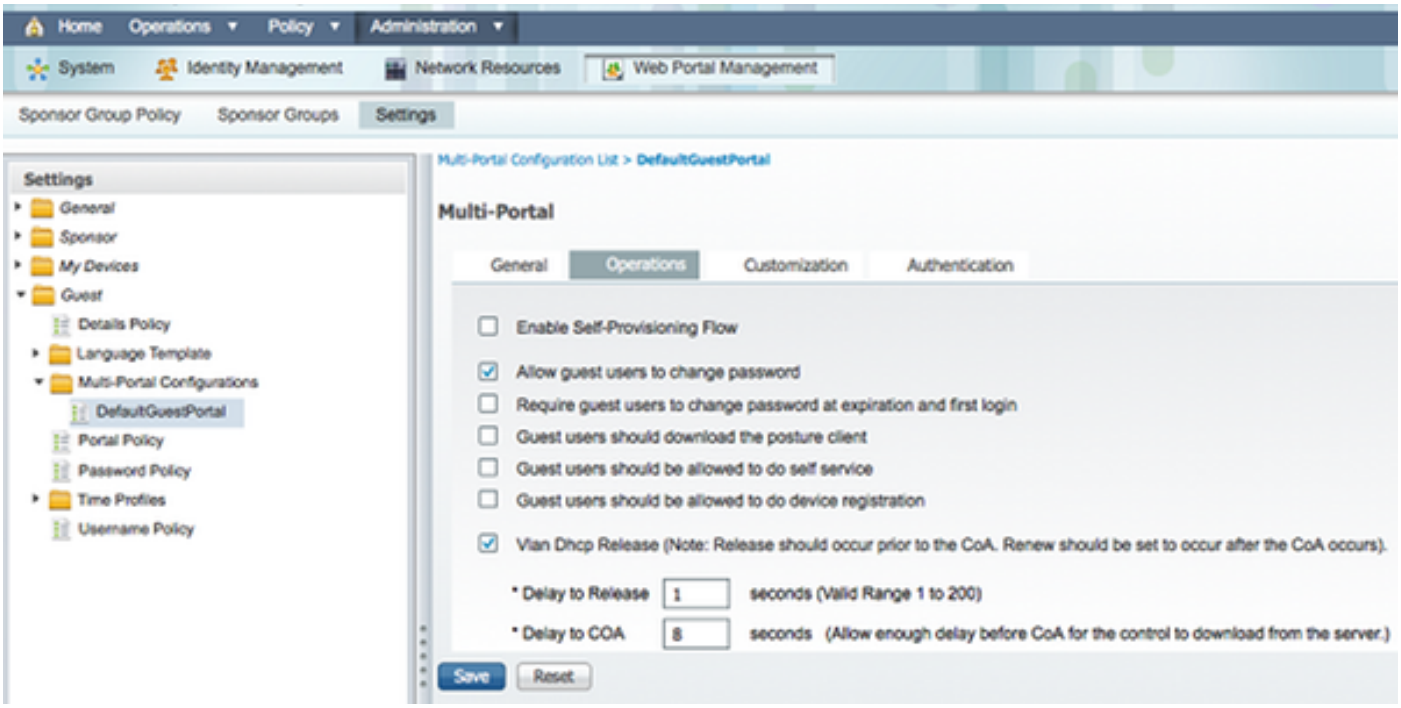
    Permit **Access** 옵션을 선택하거나 원하는 VLAN 또는 특성을 반환하기 위해 사용자 지정 프로필을 생성할 수 있습니다.

IP 갱신 활성화(선택 사항)

VLAN을 할당하는 경우 마지막 단계는 클라이언트 PC가 IP 주소를 갱신하는 것입니다.이 단계는 Windows 클라이언트용 게스트 포털에서 수행합니다.앞서 *두 번째 AUTH* 규칙에 대해 VLAN을 설정하지 않은 경우 이 단계를 건너뛸 수 있습니다.

VLAN을 할당한 경우 IP 갱신을 활성화하려면 다음 단계를 완료하십시오.

1. Administration(관리)을 클릭하고 **Guest Management(게스트 관리)**를 클릭합니다.
2. **설정**을 **클릭합니다**.
3. **Guest**를 확장하고 Multi**-Portal Configuration을 확장합니다**.
4. DefaultGuestPortal 또는 생성한 사용자 지정 포털의 이름을 클릭합니다.
5. Vlan **DHCP Releaseccheck(VLAN DHCP** 릴리스) 확인란을 클릭합니다. **참고:**이 옵션은 Windows 클라이언트에서만 작동합니다.



스위치 구성(발췌문)

이 섹션에서는 스위치 컨피그레이션의 일부를 소개합니다.전체 컨피그레이션은 스위치 컨피그레이션(전체)을 참조하십시오.

이 샘플은 간단한 MAB 컨피그레이션을 보여줍니다.

```
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 100은 전체 네트워크 연결을 제공하는 VLAN입니다.기본 포트 ACL(이름이 *webauth*)이 적용되고 아래와 같이 정의됩니다.

```
ip access-list extended webauth
permit ip any any
```

이 샘플 컨피그레이션은 사용자가 인증되지 않은 경우에도 전체 네트워크 액세스를 제공합니다.따라서 인증되지 않은 사용자에 대한 액세스를 제한할 수 있습니다.

이 컨피그레이션에서는 ISE가 리디렉션 ACL(명명된 리디렉션)을 사용하도록 구성되어 있으므로 HTTP 및 HTTPS 브라우징이 인증 없이 작동하지 않습니다(다른 ACL에 따라). 스위치의 정의는 다음과 같습니다.

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

```
permit TCP any any eq 443
```
스위치가 리디렉션을 수행할 트래픽을 정의하려면 스위치에 이 액세스 목록을 정의해야 합니다.(*허가에 일치합니다.*) 이 예에서는 클라이언트가 전송하는 모든 HTTP 또는 HTTPS 트래픽이 웹 리디렉션을 트리거합니다.또한 이 예에서는 ISE IP 주소를 거부하므로 ISE로 가는 트래픽이 ISE로 이동하며 루프에서 리디렉션되지 않습니다.(이 시나리오에서는 deny가 트래픽을 차단하지 않습니다.트래픽을 리디렉션하지 않습니다.) 비정상적인 HTTP 포트 또는 프록시를 사용하는 경우 다른 포트를 추가할 수 있습니다.

또 다른 가능성은 일부 웹 사이트에 대한 HTTP 액세스를 허용하고 다른 웹 사이트를 리디렉션하는 것입니다.예를 들어 ACL에서 내부 웹 서버에 대한 허용만 정의하는 경우 클라이언트는 인증을 받지 않고 웹을 탐색할 수 있지만 내부 웹 서버에 액세스하려고 하면 리디렉션이 발생합니다.

마지막 단계는 스위치에서 CoA를 허용하는 것입니다.그렇지 않으면 ISE는 스위치가 클라이언트를 재인증하도록 강제할 수 없습니다.

```
aaa server radius dynamic-author
client <ISE ip address> server-key <radius shared secret>
```
HTTP 트래픽을 기반으로 스위치를 리디렉션하려면 이 명령이 필요합니다.

```
ip http server
```
HTTPS 트래픽을 기반으로 리디렉션하려면 이 명령이 필요합니다.

```
ip http secure-server
```
다음 명령도 중요합니다.

```
radius-server vsa send authentication
radius-server vsa send accounting
```
사용자가 아직 인증되지 않은 경우 **show authentication session int <interface num>은** 다음 출력을 반환합니다.

```
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
```

참고:MAB 인증에 성공했지만 ISE에서 MAC 주소를 알 수 없으므로 리디렉션 ACL이 배치됩니다.

스위치 구성(전체)

이 섹션에서는 전체 스위치 구성을 보여줍니다.일부 불필요한 인터페이스와 명령줄이 생략되었습니다.따라서 이 샘플 컨피그레이션은 참조용으로만 사용해야 하며 복사해서는 안 됩니다.

```
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 프록시 컨피그레이션

클라이언트에 대해 HTTP 프록시를 사용하는 경우, 이는 클라이언트가 다음과 같은 것을 의미합니다.

- HTTP 프로토콜에 비정규 포트 사용
- 모든 트래픽을 해당 프록시로 전송

스위치가 비정규화 포트(예: 8080)에서 수신하도록 하려면 다음 명령을 사용합니다.

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

또한 프록시를 계속 사용하되 ISE IP 주소에 프록시를 사용하지 않도록 모든 클라이언트를 구성해야 합니다.모든 브라우저에는 프록시를 사용하지 않아야 하는 호스트 이름 또는 IP 주소를 입력할 수 있는 기능이 포함되어 있습니다.ISE에 대한 예외를 추가하지 않으면 루프 인증 페이지가 나타납니다.

프록시 포트(이 예에서는 8080)에서 허용하도록 리디렉션 ACL을 수정해야 합니다.

스위치 SVI에 대한 중요 참고 사항

이 시점에서 스위치에 SVI(Switch Virtual Interface)가 있어야 클라이언트에 응답하고 웹 포털 리디렉션을 클라이언트에 보낼 수 있습니다.이 SVI가 반드시 클라이언트 서브넷/VLAN에 있을 필요는 없습니다.그러나 스위치에 클라이언트 서브넷/VLAN에 SVI가 없는 경우 다른 SVI를 사용하고 클라이언트 라우팅 테이블에 정의된 대로 트래픽을 전송해야 합니다.이는 일반적으로 트래픽이 네트워크 코어의 다른 게이트웨이로 전송됨을 의미합니다.이 트래픽은 클라이언트 서브넷 내부의 액세스 스위치로 다시 돌아옵니다.

방화벽은 일반적으로 이 시나리오와 같이 동일한 스위치에서 들어오고 나가는 트래픽을 차단하므로 리디렉션이 제대로 작동하지 않을 수 있습니다.해결 방법은 방화벽에서 이 동작을 허용하거나 클라이언트 서브넷의 액세스 스위치에 SVI를 생성하는 것입니다.

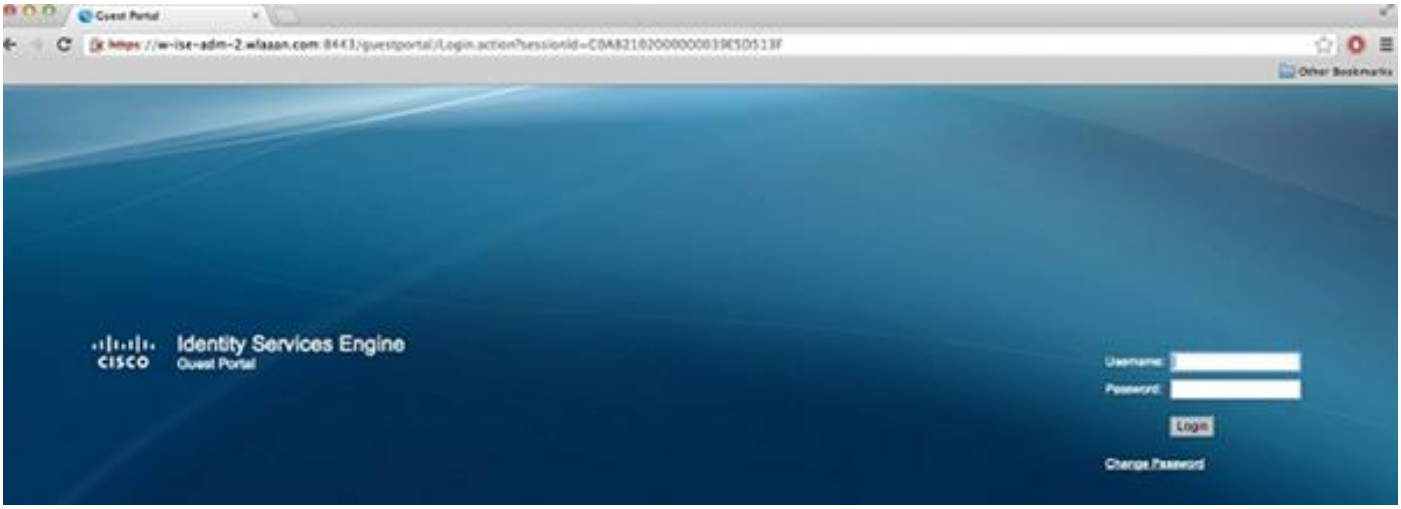
HTTPS 리디렉션에 대한 중요 참고 사항

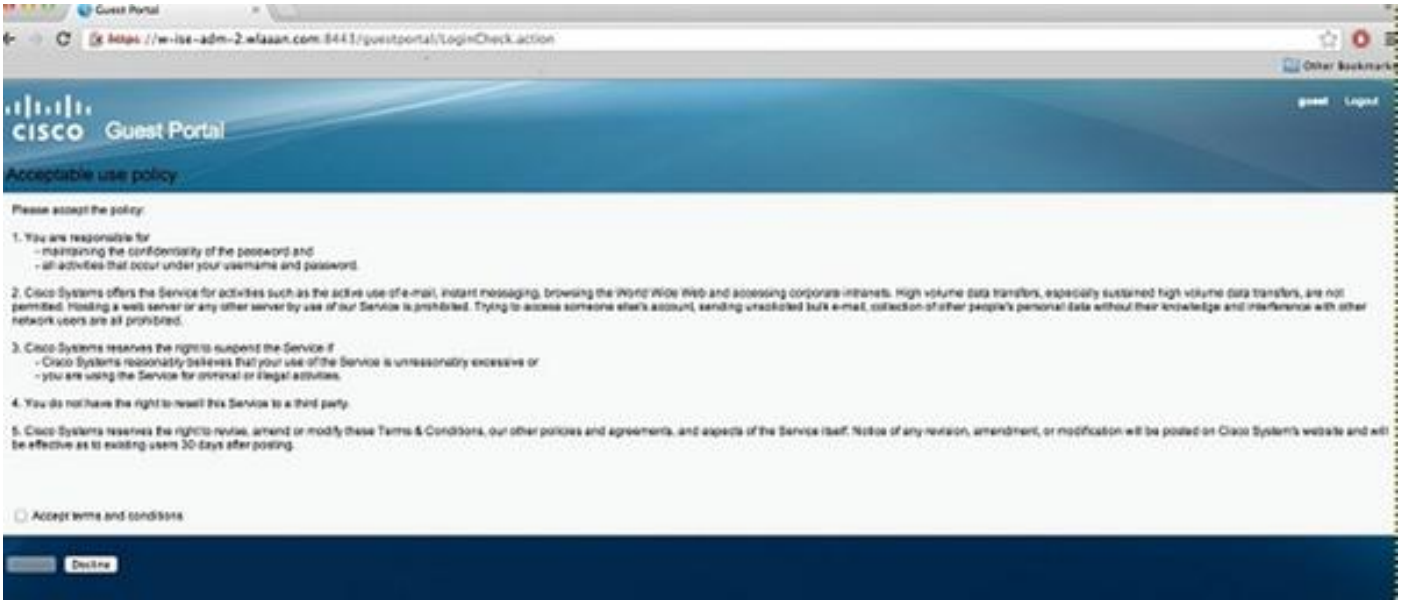
스위치는 HTTPS 트래픽을 리디렉션할 수 있습니다.따라서 게스트 클라이언트에 HTTPS에 홈 페이지가 있는 경우 리디렉션이 올바르게 수행됩니다.

리디렉션의 전체 개념은 디바이스(이 경우 스위치)가 웹 사이트 IP 주소를 스푸핑한다는 사실을 기반으로 합니다.그러나 스위치가 TLS(Transport Layer Security) 핸드셰이크에 자체 인증서만 제공할 수 있으므로 스위치가 HTTPS 트래픽을 가로채고 리디렉션하는 경우 중대한 문제가 발생합니다.이 인증서가 원래 요청된 웹 사이트와 동일하지 않으므로 대부분의 브라우저에서는 주요 경고를 발행합니다.브라우저에서는 보안 문제로 다른 인증서의 리디렉션 및 프레젠테이션을 올바르게 처리합니다.이에 대한 해결 방법은 없으며, 스위치에서 원래 웹 사이트 인증서를 스푸핑할 방법이 없습니다.

최종 결과

클라이언트 PC가 연결되고 MAB를 수행합니다.MAC 주소를 알 수 없으므로 ISE는 리디렉션 특성을 스위치에 다시 푸시합니다.사용자가 웹 사이트로 이동하려고 시도하고 리디렉션됩니다.





로그인 페이지의 인증에 성공하면 ISE는 Change Of Authorization(권한 부여 변경)을 통해 스위치 포트를 반송하며, 이는 다시 레이어 2 MAB 인증을 시작합니다.

그러나 ISE는 이전 웹 인증 클라이언트라는 것을 알고 있으며 웹 인증 자격 증명을 기반으로 클라이언트를 인증합니다(레이어 2 인증인 경우에도).

ISE 인증 로그에서 MAB 인증이 로그 하단에 나타납니다.알 수 없지만 MAC 주소가 인증되고 프로파일링되었으며 webauth 특성이 반환되었습니다.다음으로, 사용자 이름(즉, 사용자가 로그인 페이지에 자신의 자격 증명을 입력)으로 인증이 발생합니다. 인증 직후, 사용자 이름을 자격 증명으로 사용하여 새로운 레이어 2 인증이 발생합니다.이 인증 단계에서는 동적 VLAN과 같은 특성을 반환할 수 있습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Identity Services Engine
- Cisco Identity Services Engine 명령 참조 설명서
- ISE(Identity Services Engine)와 Cisco WLC(Wireless LAN Controller)의 통합
- RFC(Request for Comments)
- 기술 지원 및 문서 – Cisco Systems