Zentrale Webauthentifizierung mit einem Konfigurationsbeispiel für einen Switch und eine Identity Services Engine

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie mithilfe der Identity Services Engine (ISE) eine zentrale Webauthentifizierung für mit Switches verbundene kabelgebundene Clients konfigurieren.

Das Konzept der zentralen Web-Authentifizierung steht im Gegensatz zur lokalen Web-Authentifizierung, d. h. der üblichen Webauthentifizierung auf dem Switch selbst. Bei einem dot1x/mab-Fehler führt der Switch in diesem System ein Failover auf das Webauth-Profil durch und leitet den Client-Datenverkehr an eine Webseite auf dem Switch weiter.

Zentrale Webauthentifizierung bietet die Möglichkeit, ein zentrales Gerät zu verwenden, das als Webportal fungiert (in diesem Beispiel die ISE). Der Hauptunterschied gegenüber der üblichen lokalen Web-Authentifizierung besteht darin, dass sie zusammen mit der MAC/dot1x-Authentifizierung auf Layer 2 verschoben wird. Das Konzept unterscheidet sich auch dadurch, dass der Radius-Server (in diesem Beispiel ISE) spezielle Attribute zurückgibt, die angeben, dass eine Web-Umleitung erfolgen muss. Diese Lösung hat den Vorteil, dass Verzögerungen vermieden werden, die für die Web-Authentifizierung erforderlich sind. Wenn die MAC-Adresse der Client-Station für den Radius-Server nicht bekannt ist (aber auch andere Kriterien verwendet

werden können), gibt der Server Umleitungsattribute zurück, und der Switch autorisiert die Station (über MAB (MAC Authentication Bypass)), gibt aber eine Zugriffsliste für die Umleitung des Webdatenverkehrs zum Portal ab. Sobald sich der Benutzer im Gastportal angemeldet hat, kann der Switch-Port über CoA (Change of Authorization) mit einem Bounce zurückgesendet werden, sodass eine neue Layer-2-MAB-Authentifizierung erfolgt. Die ISE kann sich daran erinnern, dass es sich um einen Webauth-Benutzer handelte, und dem Benutzer Layer-2-Attribute (z. B. dynamische VAN-Zuweisung) zuweisen. Eine ActiveX-Komponente kann den Client-PC auch zwingen, seine IP-Adresse zu aktualisieren.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Identity Services Engine (ISE)
- Cisco IOS® Switch-Konfiguration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Identity Services Engine (ISE), Version 1.1.1
- Cisco Catalyst Switch der Serie 3560 mit Softwareversion 12.2.55SE3

  Hinweis: Das Verfahren ist bei anderen Catalyst Switch-Modellen ähnlich oder identisch. Sofern nicht anders angegeben, können Sie diese Schritte für alle Cisco IOS Software-Versionen für Catalyst verwenden.

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

Übersicht

Die ISE-Konfiguration besteht aus den folgenden fünf Schritten:

1. Erstellen Sie die herunterladbare Zugriffskontrollliste (ACL).
2. Erstellen Sie das Autorisierungsprofil.
3. Erstellen Sie eine Authentifizierungsregel.
4. Erstellen einer Autorisierungsregel.
5. Aktivieren Sie die IP-Verlängerung (optional).

Erstellen der herunterladbaren ACL

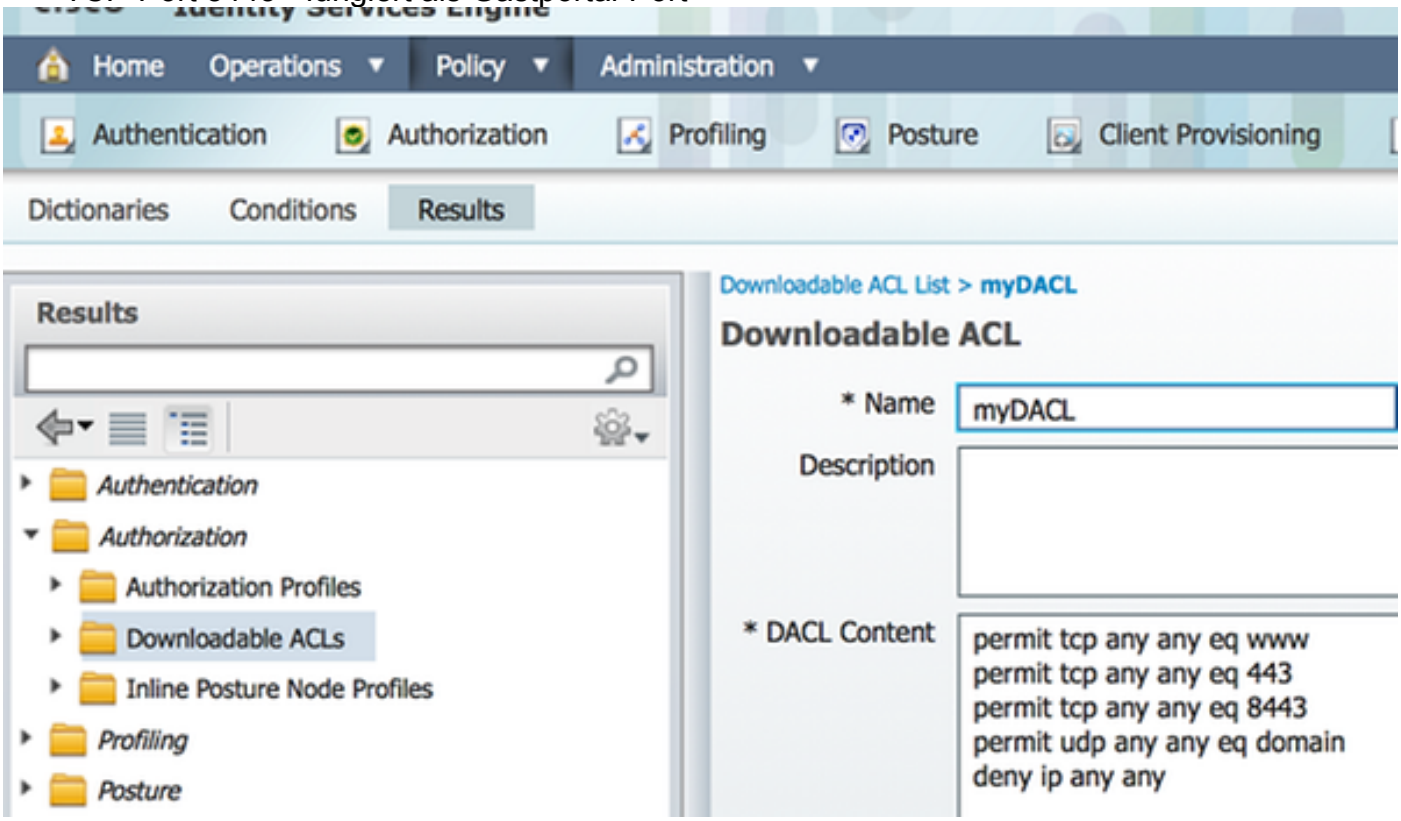
Dies ist kein obligatorischer Schritt. Die mit dem zentralen Webauth-Profil zurückgesendete umgeleitete ACL bestimmt, welcher Datenverkehr (HTTP oder HTTPS) an die ISE umgeleitet wird. Mit der herunterladbaren ACL können Sie festlegen, welcher Datenverkehr zulässig ist. Normalerweise sollten Sie DNS, HTTP(S) und 8443 zulassen und den Rest verweigern. Andernfalls leitet der Switch den HTTP-Datenverkehr um, lässt jedoch andere Protokolle zu.

Gehen Sie wie folgt vor, um die herunterladbare ACL zu erstellen:

1. Klicken Sie auf **Richtlinien** und dann auf **Richtlinienelemente**.
2. Klicken Sie auf **Ergebnisse**.
3. Erweitern Sie die **Autorisierung**, und klicken Sie auf **Herunterladbare ACLs**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**, um eine neue herunterladbare ACL zu erstellen.
5. Geben Sie im Feld **Name** einen Namen für die DACL ein. In diesem Beispiel wird *myDACL* verwendet.

Dieses Bild zeigt typischen DACL-Inhalt, der Folgendes ermöglicht:

- DNS - Auflösung des ISE-Portal-Hostnamens
- HTTP und HTTPS - Umleitung zulassen
- TCP-Port 8443 - fungiert als Gastportal-Port



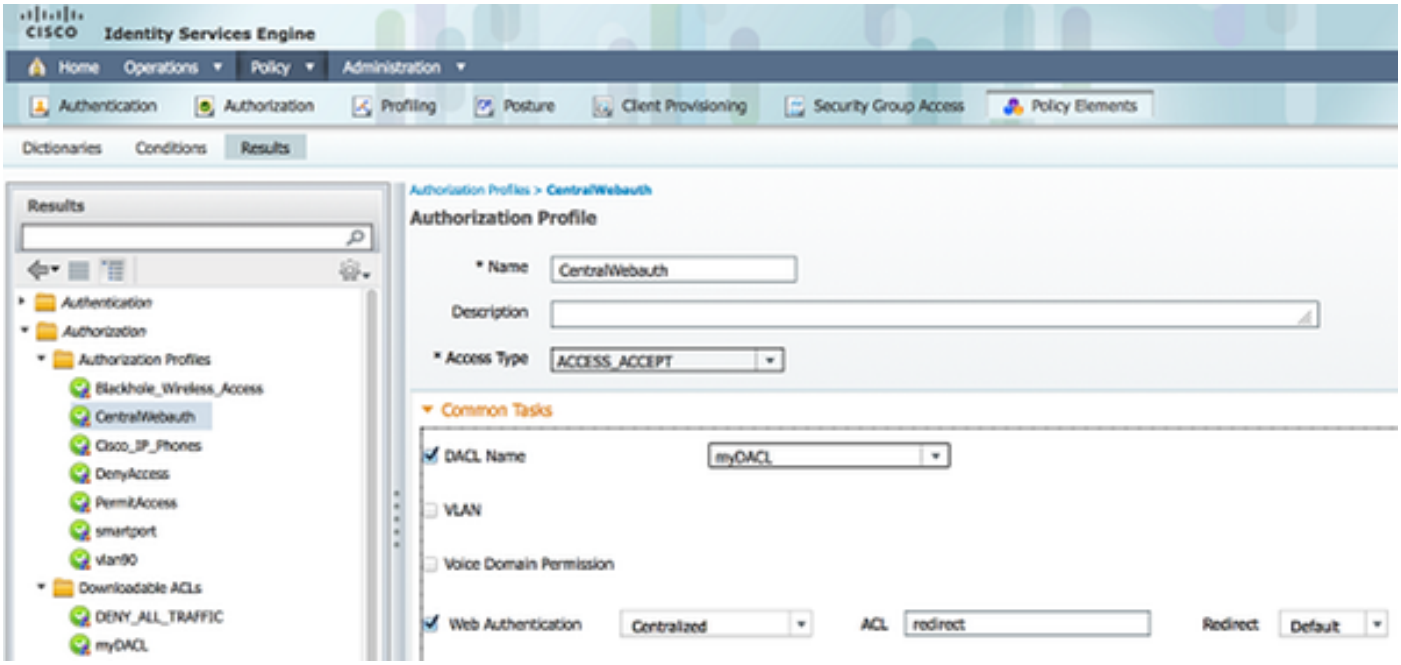
Erstellen des Autorisierungsprofils

Gehen Sie wie folgt vor, um das Autorisierungsprofil zu erstellen:

1. Klicken Sie auf **Richtlinien** und dann auf **Richtlinienelemente**.
2. Klicken Sie auf **Ergebnisse**.
3. Erweitern Sie **die Autorisierung**, und klicken Sie auf **Authorization Profile (Autorisierungsprofil)**.
4. Klicken Sie auf die Schaltfläche **Hinzufügen**, um ein neues Autorisierungsprofil für eine zentrale Webauth zu erstellen.

5. Geben Sie im Feld **Name** einen Namen für das Profil ein. In diesem Beispiel wird *CentralWebauth* verwendet.
6. Wählen Sie **ACCESS_ACCEPT** aus der Dropdown-Liste Zugriffstyp aus.
7. Aktivieren Sie das Kontrollkästchen **Webauthentifizierung**, und wählen Sie **Zentralisiert** aus der Dropdown-Liste aus.
8. Geben Sie im Feld ACL (ACL) den Namen der ACL auf dem Switch ein, die den umzuleitenden Datenverkehr definiert. In diesem Beispiel wird die *Umleitung* verwendet.
9. Wählen Sie **Default** aus der Dropdown-Liste Redirect (Umleiten) aus.
10. Aktivieren Sie das Kontrollkästchen **DACL Name**, und wählen Sie **myDACL** aus der Dropdown-Liste aus, wenn Sie eine DACL anstelle einer statischen Port-ACL am Switch verwenden möchten.

Das Redirect-Attribut definiert, ob die ISE das Standard-Webportal oder ein benutzerdefiniertes Webportal sieht, das der ISE-Administrator erstellt hat. Beispielsweise löst die *Umleitungs*-ACL in diesem Beispiel eine Umleitung für HTTP- oder HTTPS-Datenverkehr vom Client an einen beliebigen Ort aus. Die ACL wird später in diesem Konfigurationsbeispiel auf dem Switch definiert.

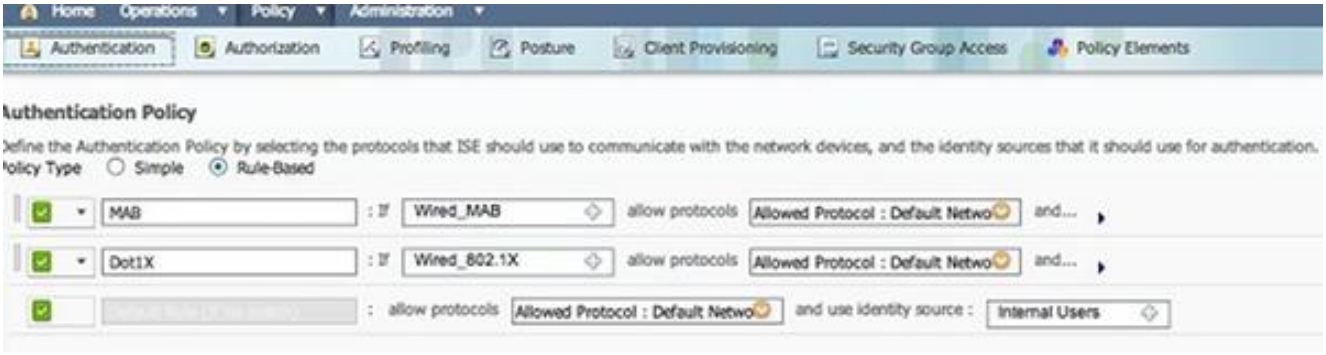


Erstellen einer Authentifizierungsregel

Gehen Sie wie folgt vor, um das Authentifizierungsprofil zum Erstellen der Authentifizierungsregel zu verwenden:

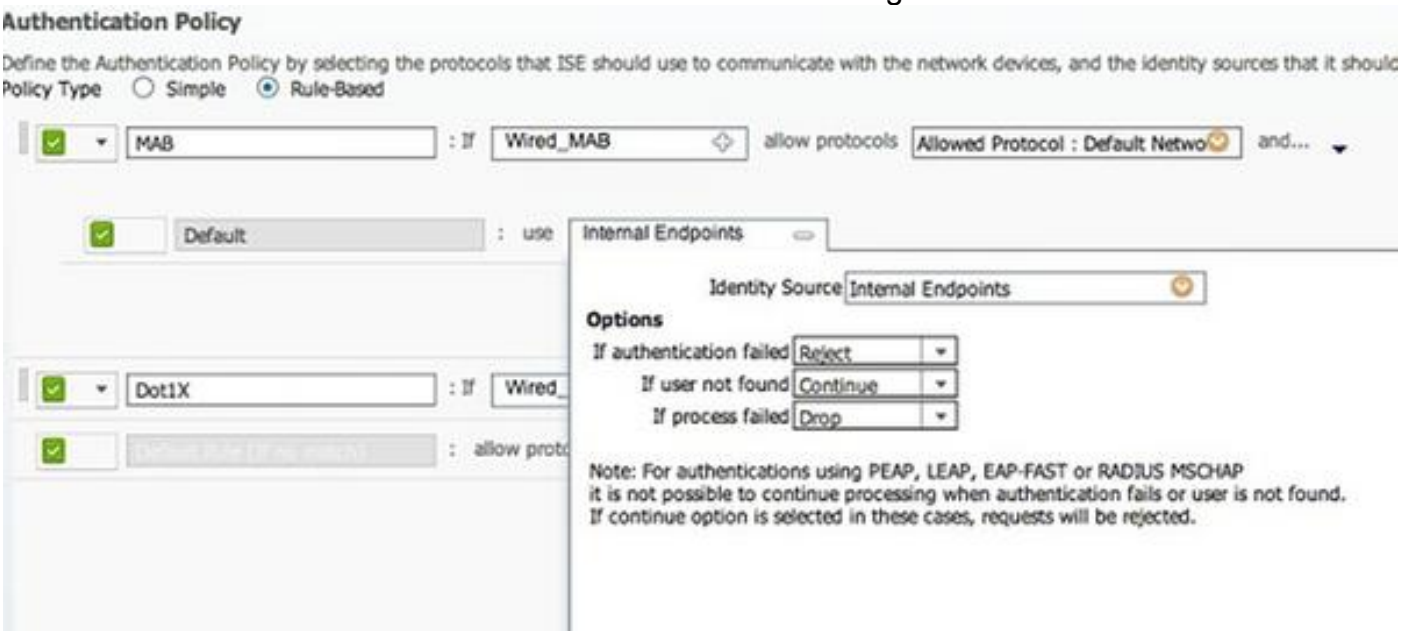
1. Klicken Sie im Menü Richtlinie auf **Authentifizierung**.

   Dieses Bild zeigt ein Beispiel für die Konfiguration der Authentifizierungsrichtlinienregel. In diesem Beispiel wird eine Regel konfiguriert, die auslöst, wenn MAB erkannt wird.



2. Geben Sie einen Namen für die Authentifizierungsregel ein. In diesem Beispiel wird *MAB* verwendet.
3. Wählen Sie das Pluszeichen (**+**) im Feld If condition aus.
4. Wählen Sie **Compound condition** (Verbundbedingung) aus, und wählen Sie **Wired_MAB aus**.
5. Klicken Sie auf den Pfeil neben **und ...** um die Regel weiter zu erweitern.
6. Klicken Sie im Feld Identitätsquelle auf das **+**-Symbol, und wählen Sie **Interne Endpunkte aus**.
7. Wählen Sie **Weiter** aus der Dropdown-Liste "Wenn der Benutzer nicht gefunden wurde" aus.

   Diese Option ermöglicht die Authentifizierung eines Geräts (über Webauth) selbst dann, wenn dessen MAC-Adresse nicht bekannt ist. Dot1x-Clients können sich immer noch mit ihren Anmeldeinformationen authentifizieren. Diese Konfiguration sollte nicht relevant sein.



Erstellen einer Autorisierungsregel

In der Autorisierungsrichtlinie müssen nun mehrere Regeln konfiguriert werden. Wenn der PC angeschlossen wird, durchläuft er die MAB-Adresse. Es wird davon ausgegangen, dass die MAC-Adresse nicht bekannt ist, sodass Webauth und ACL zurückgegeben werden. Diese *MAC*-Regel wird in diesem Bild angezeigt und in diesem Abschnitt konfiguriert:

Gehen Sie wie folgt vor, um die Autorisierungsregel zu erstellen:

1. Erstellen Sie eine neue Regel, und geben Sie einen Namen ein. In diesem Beispiel wird *MAC unbekannt* verwendet.
2. Klicken Sie im Feld Bedingung auf das Pluszeichen (**+**), und wählen Sie eine neue Bedingung aus.
3. Erweitern Sie die Dropdownliste **Ausdruck**.
4. Wählen Sie **Network Access** (Netzwerkzugriff) aus, und erweitern Sie ihn.
5. Klicken Sie auf **AuthenticationStatus**, und wählen Sie den **Equals-**Operator aus.
6. Wählen Sie **UnknownUser** im rechten Feld aus.
7. Wählen Sie auf der Seite Allgemeine Autorisierung **CentralWebauth** (Authorization Profile) im Feld rechts neben dem Wort *dann* aus.

   Mit diesem Schritt kann die ISE fortgeführt werden, auch wenn der Benutzer (oder die MAC-Adresse) nicht bekannt ist.

   Unbekannte Benutzer werden nun mit der Anmeldeseite angezeigt. Sobald sie jedoch ihre Anmeldeinformationen eingegeben haben, wird ihnen erneut eine Authentifizierungsanfrage auf der ISE angezeigt. Daher muss eine andere Regel mit einer Bedingung konfiguriert werden, die erfüllt ist, wenn der Benutzer ein Gastbenutzer ist. In diesem Beispiel wird *Wenn* die *UserIdentityGroup als Guest* verwendet wird und davon ausgegangen wird, dass alle Gäste dieser Gruppe angehören.
8. Klicken Sie auf die Aktionsschaltfläche am Ende der *MAC*-Regel, *die nicht bekannt ist*, und legen Sie oben eine neue Regel ein.

   Hinweis: Es ist sehr wichtig, dass diese neue Regel vor der *MAC*-Regel kommt, die *nicht bekannt ist*.
9. Geben Sie einen Namen für die neue Regel ein. In diesem Beispiel wird *IS-a-GUEST* verwendet.
10. Wählen Sie eine Bedingung aus, die Ihren Gastbenutzern entspricht.

    In diesem Beispiel wird *InternalUser:IdentityGroup als Guest* verwendet, da alle Gastbenutzer an die *Guest*-Gruppe (oder eine andere Gruppe, die Sie in den Sponsoreinstellungen konfiguriert haben) gebunden sind.
11. Wählen Sie **PermitAccess** im Ergebnisfeld aus (*dann* rechts neben dem Wort).

    Wenn der Benutzer auf der Anmeldeseite autorisiert ist, startet die ISE eine Layer-2-Authentifizierung auf dem Switch-Port neu, und es wird eine neue MAB-Nummer erstellt. In diesem Szenario besteht der Unterschied darin, dass für die ISE ein unsichtbares Flag festgelegt wird, um sich zu erinnern, dass es sich um einen durch Gastauthentifizierung authentifizierten Benutzer handelt. Diese Regel ist *2. AUTH*, und die Bedingung ist *Network Access:UseCase Equals GuestFlow*. Diese Bedingung wird erfüllt, wenn sich der Benutzer über Webauth authentifiziert und der Switch-Port erneut für eine neue MAB eingestellt wird. Sie können beliebige Attribute zuweisen. In diesem Beispiel wird ein Profil *vlan90* zugewiesen, sodass dem Benutzer das VLAN 90 in seiner zweiten MAB-Authentifizierung zugewiesen wird.
12. Klicken Sie auf **Aktionen** (am Ende der IS-a-GAST-Regel), und wählen Sie **Neue Regel oben einfügen aus**.
13. Geben Sie im Namensfeld **die zweite AUTH ein**.
14. Klicken Sie im Feld Bedingung auf das Pluszeichen (**+**), und wählen Sie eine neue

Bedingung aus.

15. Wählen Sie **Network Access** (Netzwerkzugriff) aus, und klicken Sie auf **UseCase**.
16. Wählen Sie **Equals** als Operator aus.
17. Wählen Sie **GuestFlow** als rechten Operanden aus.
18. Klicken Sie auf der Autorisierungsseite auf das Pluszeichen (**+**) (neben dem Symbol *dann*), um ein Ergebnis für Ihre Regel auszuwählen.

    In diesem Beispiel wird ein vorkonfiguriertes Profil (vlan90) zugewiesen. Diese Konfiguration wird in diesem Dokument nicht angezeigt.

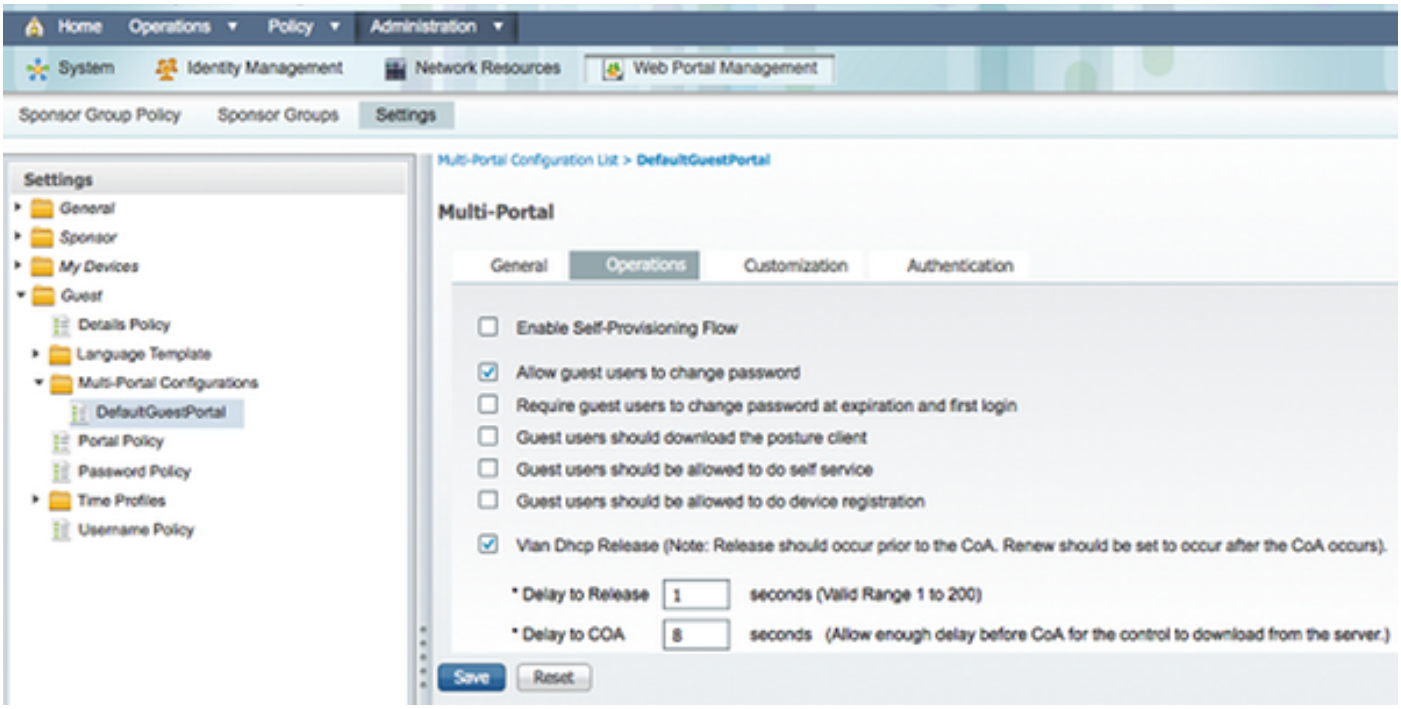
    Sie können eine **Zugriffsberechtigungsoption** auswählen oder ein benutzerdefiniertes Profil erstellen, um das VLAN oder die gewünschten Attribute zurückzugeben.

Aktivieren Sie die IP-Verlängerung (optional)

Wenn Sie ein VLAN zuweisen, muss der Client-PC seine IP-Adresse erneuern. Dieser Schritt wird über das Gastportal für Windows-Clients durchgeführt. Wenn Sie für die *zweite AUTH*-Regel kein VLAN festgelegt haben, können Sie diesen Schritt überspringen.

Wenn Sie ein VLAN zugewiesen haben, führen Sie die folgenden Schritte aus, um die IP-Verlängerung zu aktivieren:

1. Klicken Sie auf **Administration** und dann auf **Guest Management**.
2. Klicken Sie auf **Einstellungen**.
3. Erweitern Sie **Guest** und erweitern Sie **Multi-Portal Configuration**.
4. Klicken Sie auf **DefaultGuestPortal** oder den Namen eines benutzerdefinierten Portals, das Sie möglicherweise erstellt haben.
5. Klicken Sie auf das Kontrollkästchen **VLAN DHCP Releasecheck**. **Hinweis**: Diese Option funktioniert nur für Windows-Clients.



Switch-Konfiguration (Excerpt)

Dieser Abschnitt enthält einen Auszug aus der Switch-Konfiguration. Die vollständige Konfiguration finden Sie unter Switch-Konfiguration (Voll).

Dieses Beispiel zeigt eine einfache MAB-Konfiguration.

```
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 100 ist das VLAN, das vollständige Netzwerkverbindungen bereitstellt. Eine Standard-Port-ACL (*webauth* genannt) wird angewendet und wie folgt definiert:

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

Diese Beispielkonfiguration bietet vollen Netzwerkzugriff, selbst wenn der Benutzer nicht authentifiziert ist. Daher sollten Sie den Zugriff auf nicht authentifizierte Benutzer einschränken.

In dieser Konfiguration funktioniert das HTTP- und HTTPS-Browsen nicht ohne Authentifizierung (über die andere ACL), da die ISE für die Verwendung einer Umleitungszugriffskontrollliste (mit dem Namen *Redirect*) konfiguriert ist. Die Definition auf dem Switch lautet wie folgt:

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

Diese Zugriffsliste muss auf dem Switch definiert werden, um festzulegen, für welchen Datenverkehr der Switch die Umleitung durchführen soll. (Übereinstimmung mit *Genehmigung*.) In diesem Beispiel löst jeder HTTP- oder HTTPS-Datenverkehr, den der Client sendet, eine Web-Umleitung aus. In diesem Beispiel wird auch die ISE-IP-Adresse abgelehnt, sodass der Datenverkehr zur ISE an die ISE weitergeleitet wird und nicht in einer Schleife umgeleitet wird. (In diesem Szenario wird der Datenverkehr durch "deny" nicht blockiert. wird der Datenverkehr nicht umgeleitet.) Wenn Sie ungewöhnliche HTTP-Ports oder einen Proxy verwenden, können Sie weitere Ports hinzufügen.

Eine weitere Möglichkeit besteht darin, HTTP-Zugriff auf einige Websites zuzulassen und andere Websites umzuleiten. Wenn Sie z. B. in der ACL eine Genehmigung nur für interne Webserver definieren, können Clients das Internet durchsuchen, ohne sich zu authentifizieren, aber die Umleitung würde erfolgen, wenn sie versuchen, auf einen internen Webserver zuzugreifen.

Der letzte Schritt besteht darin, CoA auf dem Switch zuzulassen. Andernfalls kann die ISE den Switch nicht zwingen, den Client erneut zu authentifizieren.

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

Dieser Befehl ist für die Umleitung des Switches basierend auf dem HTTP-Datenverkehr

erforderlich:

```
ip http server
```

Dieser Befehl ist für die Umleitung auf Basis von HTTPS-Datenverkehr erforderlich:

```
ip http secure-server
```

Diese Befehle sind ebenfalls wichtig:

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

Wenn der Benutzer noch nicht authentifiziert ist, gibt die **show authentication session int <interface num>** diese Ausgabe zurück:

```
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
```

Hinweis: Trotz erfolgreicher MAB-Authentifizierung wird die Umleitungs-ACL platziert, da die MAC-Adresse von der ISE nicht bekannt war.

Switch-Konfiguration (vollständig)

In diesem Abschnitt wird die vollständige Switch-Konfiguration aufgeführt. Einige unnötige Schnittstellen und Befehlszeilen wurden weggelassen. Daher sollte diese Beispielkonfiguration nur als Referenz verwendet und nicht kopiert werden.

```
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-Proxy-Konfiguration

Wenn Sie einen HTTP-Proxy für Ihre Clients verwenden, bedeutet dies, dass Ihre Clients:

- Verwendung eines unkonventionellen Ports für HTTP-Protokoll
- Senden Sie den gesamten Datenverkehr an diesen Proxy.

Um den Switch am unkonventionellen Port abhören zu lassen (z. B. 8080), verwenden Sie die folgenden Befehle:

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

Sie müssen auch alle Clients so konfigurieren, dass sie ihren Proxy weiterhin verwenden, jedoch nicht den Proxy für die ISE-IP-Adresse verwenden. Alle Browser enthalten eine Funktion, mit der Sie Hostnamen oder IP-Adressen eingeben können, die den Proxy nicht verwenden sollten. Wenn Sie die Ausnahme für die ISE nicht hinzufügen, wird eine Seite zur Schleifenauthentifizierung angezeigt.

Sie müssen außerdem die Umleitungs-ACL so ändern, dass sie auf dem Proxyport zugelassen wird (in diesem Beispiel 8080).

Wichtiger Hinweis zu Switch-SVIs

Zu diesem Zeitpunkt benötigt der Switch eine virtuelle Switch-Schnittstelle (SVI), um auf den Client zu antworten und die Umleitung des Webportals an den Client zu senden. Diese SVI muss sich nicht unbedingt im Subnetz/VLAN des Clients befinden. Wenn der Switch jedoch keine SVI im Client-Subnetz/VLAN hat, muss er eine der anderen SVIs verwenden und Datenverkehr gemäß der Definition in der Client-Routing-Tabelle senden. Dies bedeutet in der Regel, dass Datenverkehr an ein anderes Gateway im Netzwerkkern gesendet wird. dieser Datenverkehr wird zurück zum Access Switch im Client-Subnetz geleitet.

Firewalls blockieren in der Regel den Datenverkehr vom und zum selben Switch, wie in diesem Szenario, sodass eine Umleitung möglicherweise nicht ordnungsgemäß funktioniert. Workarounds

sollen dieses Verhalten auf der Firewall erlauben oder eine SVI auf dem Access Switch im Client-Subnetz erstellen.

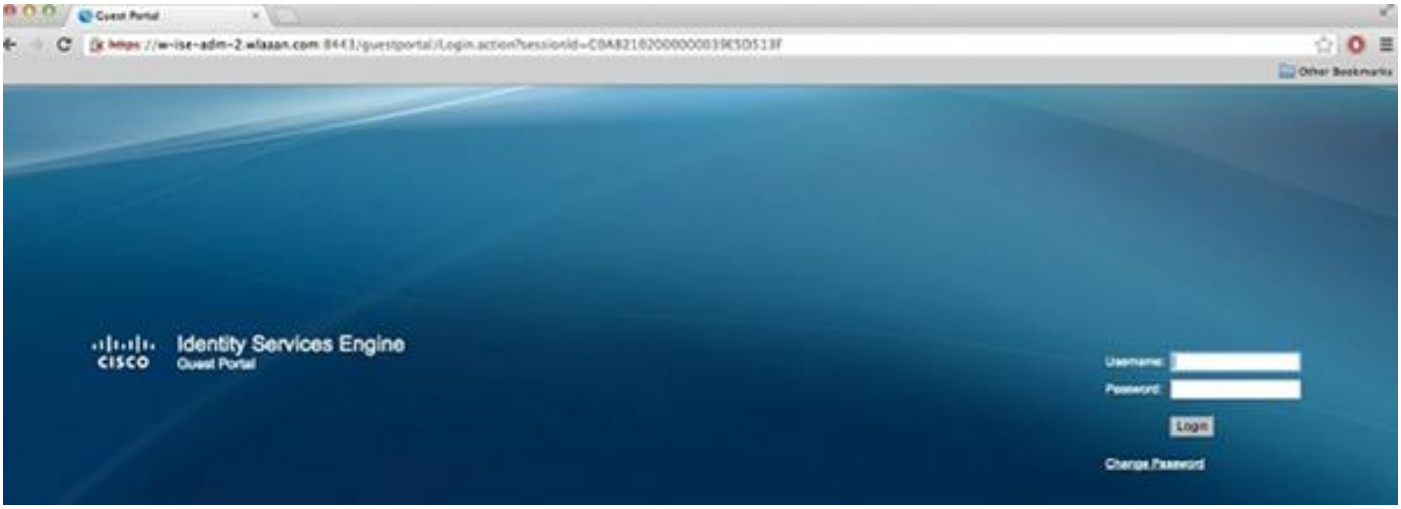
Wichtiger Hinweis zur HTTPS-Umleitung

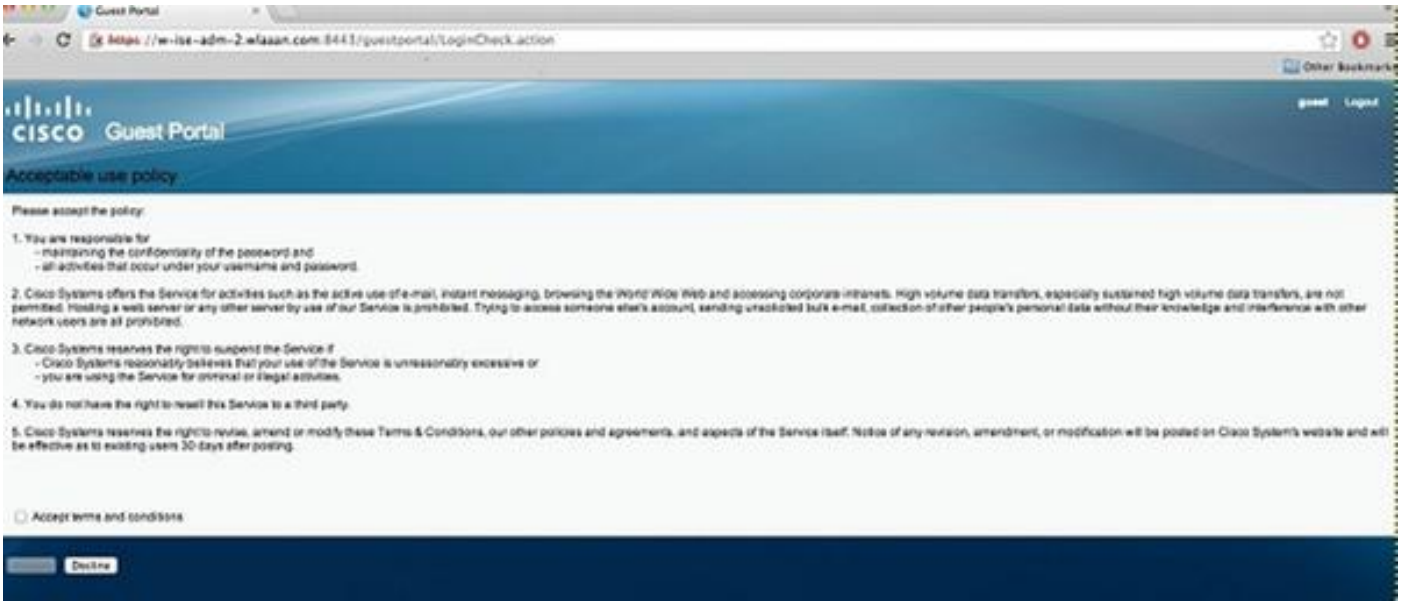
Switches können HTTPS-Datenverkehr umleiten. Wenn der Gast-Client über eine HTTPS-Startseite verfügt, wird die Umleitung also korrekt durchgeführt.

Das gesamte Konzept der Umleitung basiert auf der Tatsache, dass ein Gerät (in diesem Fall der Switch) die IP-Adresse der Website abruft. Beim Abfangen und Umleiten von HTTPS-Datenverkehr durch den Switch tritt jedoch ein großes Problem auf, da der Switch im Transport Layer Security (TLS)-Handshake nur sein eigenes Zertifikat präsentieren kann. Da es sich hierbei nicht um dasselbe Zertifikat wie die ursprünglich angeforderte Website handelt, geben die meisten Browser wichtige Warnmeldungen aus. Die Browser behandeln die Umleitung und Präsentation eines anderen Zertifikats als Sicherheitsproblem korrekt. Dafür gibt es keine Lösung, und es gibt keine Möglichkeit, dass der Switch Ihr ursprüngliches Webseitenzertifikat verfälscht.

Endergebnis

Der Client-PC wird angeschlossen und führt MAB aus. Da die MAC-Adresse nicht bekannt ist, überträgt die ISE die Umleitungsattribute zurück an den Switch. Der Benutzer versucht, eine Website zu öffnen und wird umgeleitet.





Wenn die Authentifizierung der Anmeldeseite erfolgreich ist, setzt die ISE den Switch-Port durch "Change Of Authorization" (Autorisierungsänderung ändern) frei, wodurch wiederum eine Layer-2-MAB-Authentifizierung gestartet wird.

Die ISE weiß jedoch, dass es sich um einen früheren Webauth-Client handelt, der den Client anhand der Webauth-Anmeldeinformationen autorisiert (obwohl es sich um eine Layer-2-Authentifizierung handelt).

In den ISE-Authentifizierungsprotokollen wird unten im Protokoll die MAB-Authentifizierung angezeigt. Obwohl es unbekannt ist, wurde die MAC-Adresse authentifiziert und mit einem Profil versehen, und die Webauth-Attribute wurden zurückgegeben. Anschließend wird die Authentifizierung mit dem Benutzernamen des Benutzers durchgeführt (d. h. der Benutzer gibt seine Anmeldeinformationen auf der Anmeldeseite ein). Unmittelbar nach der Authentifizierung erfolgt eine neue Layer-2-Authentifizierung mit dem Benutzernamen als Anmeldeinformationen. In diesem Authentifizierungsschritt können Sie Attribute wie dynamisches VLAN zurückgeben.

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

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

Zugehörige Informationen

- Cisco Identity Services Engine
- Cisco Identity Services Engine - Befehlsreferenz
- Integration der ISE (Identity Services Engine) mit dem Cisco WLC (Wireless LAN Controller)
- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation - Cisco Systems