Esempio di autenticazione Web centrale con uno switch e configurazione di Identity Services Engine

Sommario

Introduzione

Questo documento descrive come configurare l'autenticazione Web centrale con i client cablati connessi agli switch con l'aiuto di Identity Services Engine (ISE).

Il concetto di autenticazione Web centrale è contrario all'autenticazione Web locale, che è la consueta autenticazione Web sullo switch stesso. In questo sistema, in caso di errore dot1x/mab, lo switch eseguirà il failover sul profilo webauth e reindirizzerà il traffico dei client a una pagina Web sullo switch.

L'autenticazione Web centrale offre la possibilità di avere un dispositivo centrale che funge da portale Web (nell'esempio, l'ISE). La differenza principale rispetto alla normale autenticazione Web locale consiste nel fatto che viene spostata sul layer 2 insieme all'autenticazione mac/dot1x. Il concetto differisce anche nel fatto che il server radius (ISE in questo esempio) restituisce attributi speciali che indicano allo switch che deve essere eseguito un reindirizzamento Web. Questa soluzione ha il vantaggio di eliminare qualsiasi ritardo necessario per l'autenticazione Web. A livello globale, se l'indirizzo MAC della stazione client non è noto al server radius (ma è possibile utilizzare anche altri criteri), il server restituisce gli attributi di reindirizzamento e lo switch

autorizza la stazione (tramite MAC Authentication Bypass [MAB]) ma inserisce un elenco degli accessi per reindirizzare il traffico Web al portale. Una volta che l'utente ha effettuato l'accesso al portale guest, è possibile, tramite CoA (Change of Authorization), far rimbalzare la porta dello switch in modo che si verifichi una nuova autenticazione MAB di layer 2. L'ISE ricorda di essere un utente webauth e applica all'utente gli attributi di layer 2 (come l'assegnazione dinamica di VLAN). Un componente ActiveX può inoltre forzare il PC client ad aggiornare il proprio indirizzo IP.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Identity Services Engine (ISE)
- Configurazione switch Cisco IOS®

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco Identity Services Engine (ISE), versione 1.1.1
- Cisco Catalyst serie 3560 Switch con software versione 12.2.55SE3

  Nota: la procedura è simile o identica per altri modelli di switch Catalyst. Se non specificato diversamente, è possibile eseguire la procedura seguente su tutte le versioni del software Cisco IOS per Catalyst.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Panoramica

La configurazione ISE è composta dalle seguenti cinque fasi:

1. Creare l'elenco di controllo di accesso (ACL) scaricabile.
2. Creare il profilo di autorizzazione.
3. Creare una regola di autenticazione.
4. Creare una regola di autorizzazione.
5. Abilitare il rinnovo IP (facoltativo).

Creazione dell'ACL scaricabile

Questa operazione non è obbligatoria. L'ACL di reindirizzamento inviato con il profilo webauth

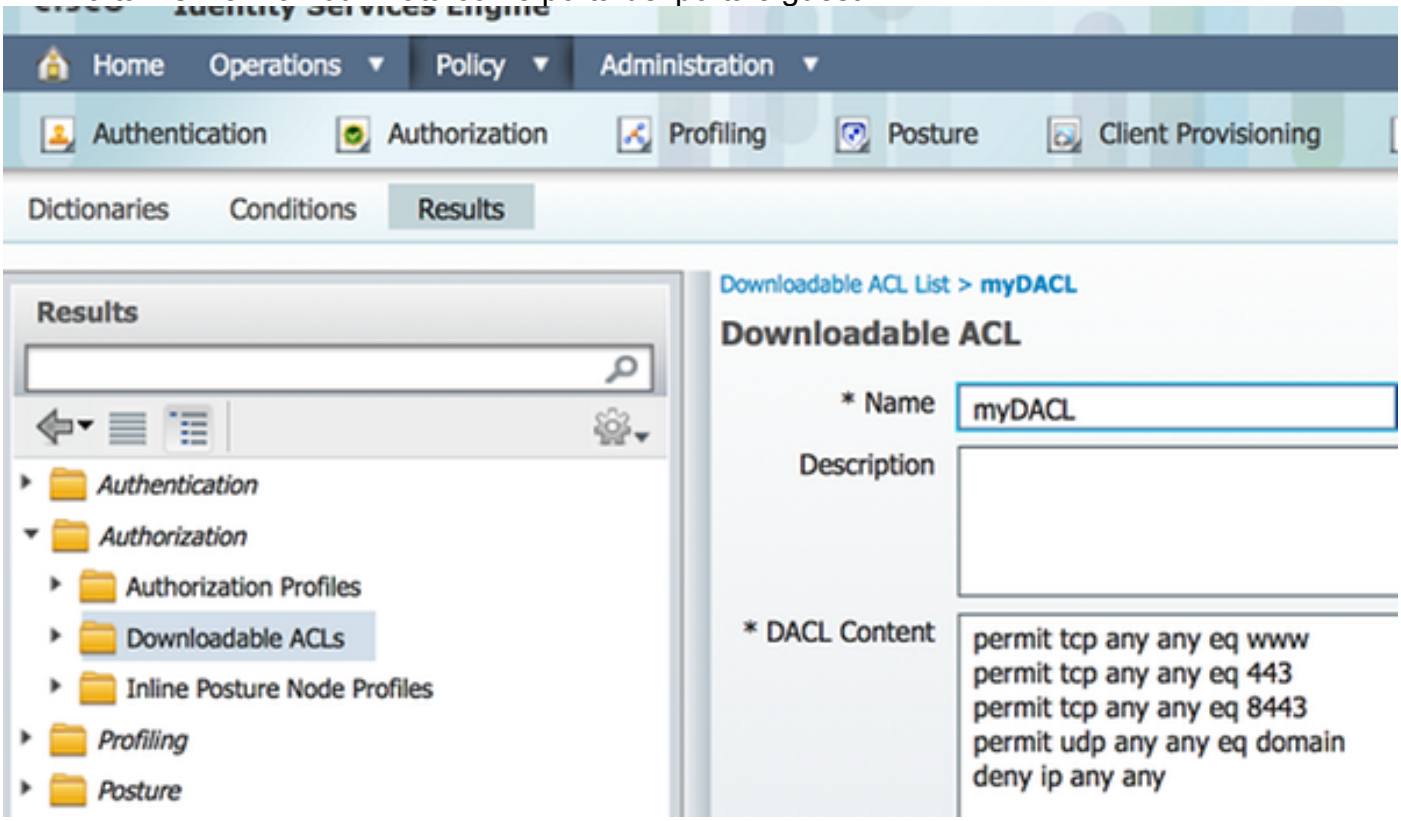
centrale determina quale traffico (HTTP o HTTPS) viene reindirizzato all'ISE. L'ACL scaricabile permette di definire il traffico consentito. È consigliabile in genere consentire DNS, HTTP(S) e 8443 e negare il resto. In caso contrario, lo switch reindirizza il traffico HTTP ma consente altri protocolli.

Completare questa procedura per creare l'ACL scaricabile:

1. Fare clic su **Criterio**, quindi su **Elementi criterio**.
2. Fare clic su **Risultati**.
3. Espandere **Authorization** (Autorizzazione), quindi fare clic su **Downloadable ACLs** (ACL scaricabili).
4. Per creare un nuovo ACL scaricabile, fare clic sul pulsante **Add** (Aggiungi).
5. Nel campo **Name** (Nome), immettere un nome per l'elenco DACL. In questo esempio viene utilizzato *myDACL*.

Questa immagine mostra il contenuto DACL tipico, che consente:

- DNS - risoluzione del nome host del portale ISE
- HTTP e HTTPS - consenti reindirizzamento
- Porta TCP 8443 - utilizzata come porta del portale guest



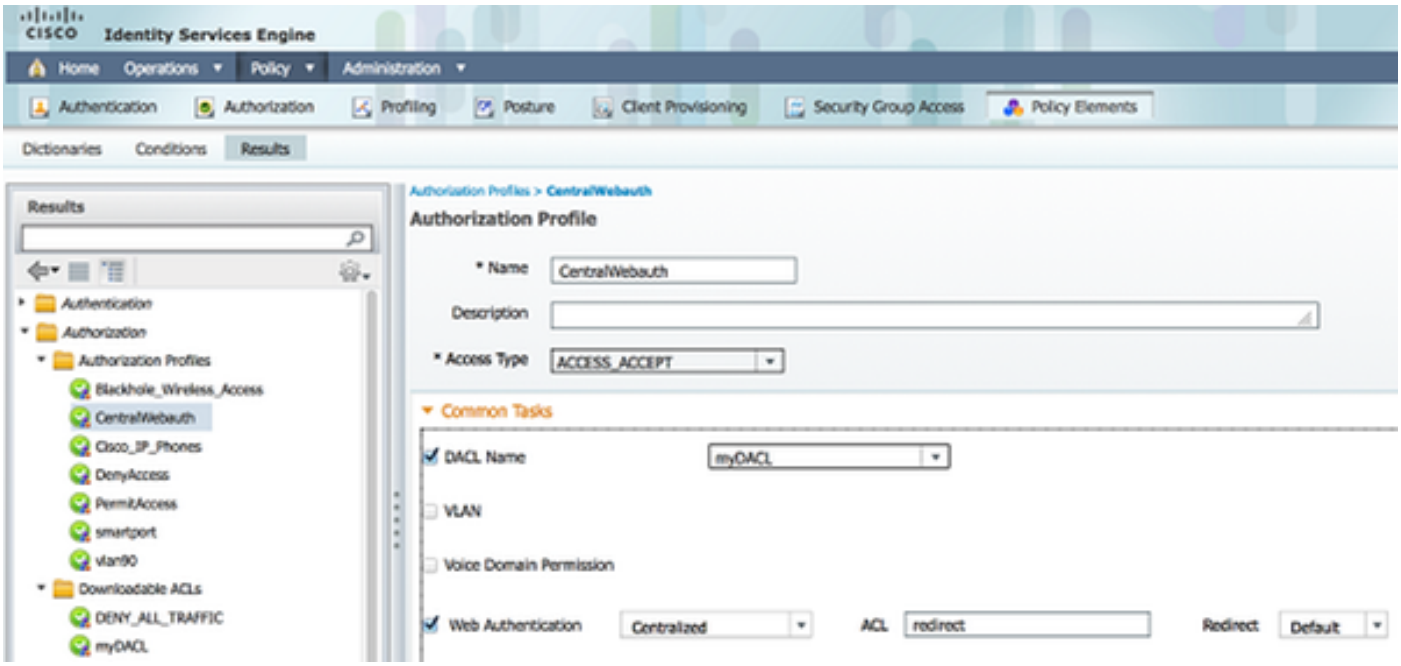
Creazione del profilo di autorizzazione

Per creare il profilo di autorizzazione, completare i seguenti passaggi:

1. Fare clic su **Criterio**, quindi su **Elementi criterio**.
2. Fare clic su **Risultati**.
3. Espandere **Autorizzazione** e fare clic su **Profilo autorizzazione**.
4. Per creare un nuovo profilo di autorizzazione per webauth centrale, fare clic sul pulsante **Add** (Aggiungi).

5. Nel campo **Nome**, immettere un nome per il profilo. In questo esempio viene utilizzato *CentralWebauth*.
6. Selezionare **ACCESS_ACCEPT** dall'elenco a discesa Access Type.
7. Selezionare la casella di controllo **Autenticazione Web** e scegliere **Centralizzata** dall'elenco a discesa.
8. Nel campo ACL, immettere il nome dell'ACL sullo switch che definisce il traffico da reindirizzare. In questo esempio viene utilizzato il *reindirizzamento*.
9. Selezionare **Predefinito** dall'elenco a discesa Reindirizza.
10. Selezionare la casella di controllo **Nome DACL** e scegliere **myDACL** dall'elenco a discesa se si decide di utilizzare un DACL anziché un ACL con porta statica sullo switch.

L'attributo Redirect definisce se l'ISE deve vedere il portale Web predefinito o un portale Web personalizzato creato dall'amministratore ISE. Ad esempio, l'ACL di *reindirizzamento* illustrato in questo esempio attiva un reindirizzamento sul traffico HTTP o HTTPS dal client a qualsiasi posizione. L'ACL viene definito sullo switch più avanti in questo esempio di configurazione.

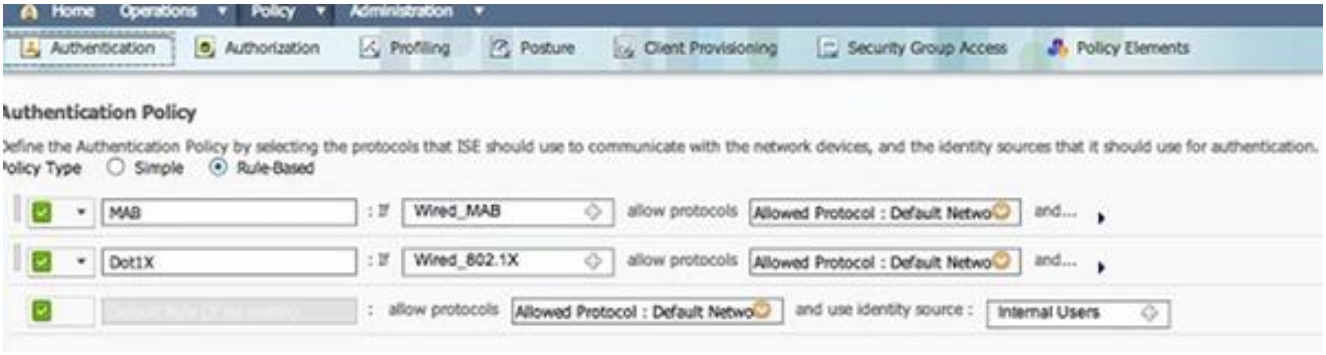


Creare una regola di autenticazione

Per utilizzare il profilo di autenticazione per creare la regola di autenticazione, completare la procedura seguente:

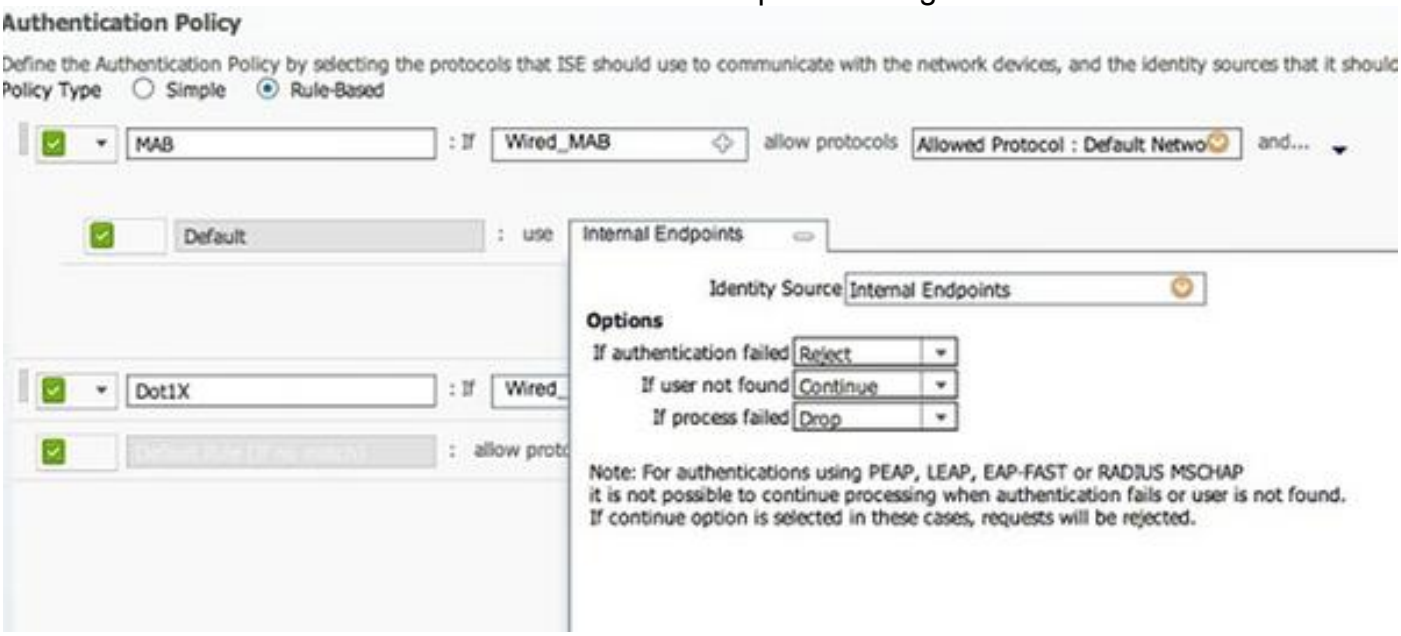
1. Scegliere **Autenticazione** dal menu Criteri.

   In questa immagine viene illustrato un esempio di come configurare la regola dei criteri di autenticazione. In questo esempio viene configurata una regola che viene attivata quando viene rilevato MAB.



2. Immettere un nome per la regola di autenticazione. In questo esempio viene utilizzato *MAB*.
3. Selezionare l'icona più (**+**) nel campo Condizione If.
4. Selezionate **Condizione composta (Compound condition)**, quindi **Wired_MAB**.
5. Fare clic sulla freccia accanto a **e ...** per espandere ulteriormente la regola.
6. Fare clic sull'icona **+** nel campo Origine identità e scegliere **Endpoint interni**.
7. Scegliere **Continua** dall'elenco a discesa "Se l'utente non è stato trovato".

   Questa opzione consente di autenticare un dispositivo (tramite webauth) anche se il relativo indirizzo MAC non è noto. I client Dot1x possono ancora eseguire l'autenticazione con le credenziali e non devono essere interessati da questa configurazione.



Creare una regola di autorizzazione

Sono ora disponibili diverse regole da configurare nei criteri di autorizzazione. Quando il PC è collegato alla rete elettrica, passa attraverso MAB; si presume che l'indirizzo MAC non sia noto, quindi vengono restituiti webauth e ACL. Questa regola *MAC sconosciuto* è mostrata in questa immagine ed è configurata in questa sezione:

Per creare la regola di autorizzazione, completare i seguenti passaggi:

1. Creare una nuova regola e immettere un nome. In questo esempio viene utilizzato un

indirizzo MAC sconosciuto.
2. Fare clic sul pulsante più (**+**) nel campo condizione e scegliere di creare una nuova condizione.
3. Espandere l'elenco a discesa **espressione**.
4. Scegliere **Accesso alla rete** ed espanderlo.
5. Fare clic su **AuthenticationStatus**, quindi scegliere l'operatore **Equals**.
6. Scegliere **UnknownUser** (Utente sconosciuto) nel campo di destra.
7. Nella pagina Autorizzazione generale, scegliere **CentralWebauth** (Profilo di autorizzazione) nel campo a destra della parola *quindi*.

   Questo passaggio consente all'ISE di continuare anche se l'utente (o l'MAC) non è noto.

   Agli utenti sconosciuti viene ora visualizzata la pagina Accesso. Tuttavia, una volta immesse le credenziali, l'utente viene nuovamente presentato con una richiesta di autenticazione all'ISE; pertanto, un'altra regola deve essere configurata con una condizione che viene soddisfatta se l'utente è un utente guest. In questo esempio, *se UseridentityGroup è uguale a Guest* viene utilizzato e si presuppone che tutti gli utenti guest appartengano a questo gruppo.
8. Fare clic sul pulsante delle azioni situato alla fine della regola *MAC sconosciuto* e scegliere di inserire una nuova regola.

   Nota: È molto importante che questa nuova regola venga prima della regola *MAC sconosciuto*.
9. Immettere un nome per la nuova regola. In questo esempio viene utilizzato *IS-a-GUEST*.
10. Scegliere una condizione corrispondente agli utenti guest.

    In questo esempio viene utilizzato *InternalUser:IdentityGroup Equals Guest* perché tutti gli utenti guest sono associati al gruppo *Guest* o a un altro gruppo configurato nelle impostazioni dello sponsor.
11. Scegliere **PermitAccess** nella casella dei risultati (a destra della parola *quindi*).

    Quando l'utente è autorizzato nella pagina Login, ISE riavvia l'autenticazione di layer 2 sulla porta dello switch e si verifica un nuovo MAB. In questo scenario, la differenza è che per ISE è impostato un flag invisibile per ricordare che si trattava di un utente autenticato come guest. Questa regola è la *seconda autenticazione* e la condizione è *Accesso di rete: UseCase è uguale a GuestFlow*. Questa condizione viene soddisfatta quando l'utente esegue l'autenticazione tramite webauth e la porta dello switch viene impostata di nuovo per un nuovo MAB. È possibile assegnare gli attributi desiderati. In questo esempio viene assegnato un profilo *vlan90* in modo che all'utente venga assegnata la VLAN 90 nella seconda autenticazione MAB.
12. Fare clic su **Azioni** (posizionato alla fine della regola IS-a-GUEST) e scegliere **Inserisci nuova regola sopra**.
13. Immettere **2a AUTH** nel campo del nome.
14. Nel campo condizione, fare clic sul più (**+**) icona e scegliere di creare una nuova condizione.
15. Scegliere **Accesso alla rete** e fare clic su **UseCase**.
16. Selezionare **Uguale** come operatore.
17. Scegliere **GuestFlow** come operando destro.

18. Nella pagina di autorizzazione, fare clic sul pulsante più (**+**) accanto a *quindi* per scegliere un risultato per la regola.

    nell'esempio, viene assegnato un profilo preconfigurato (vlan90); questa configurazione non viene visualizzata nel documento.

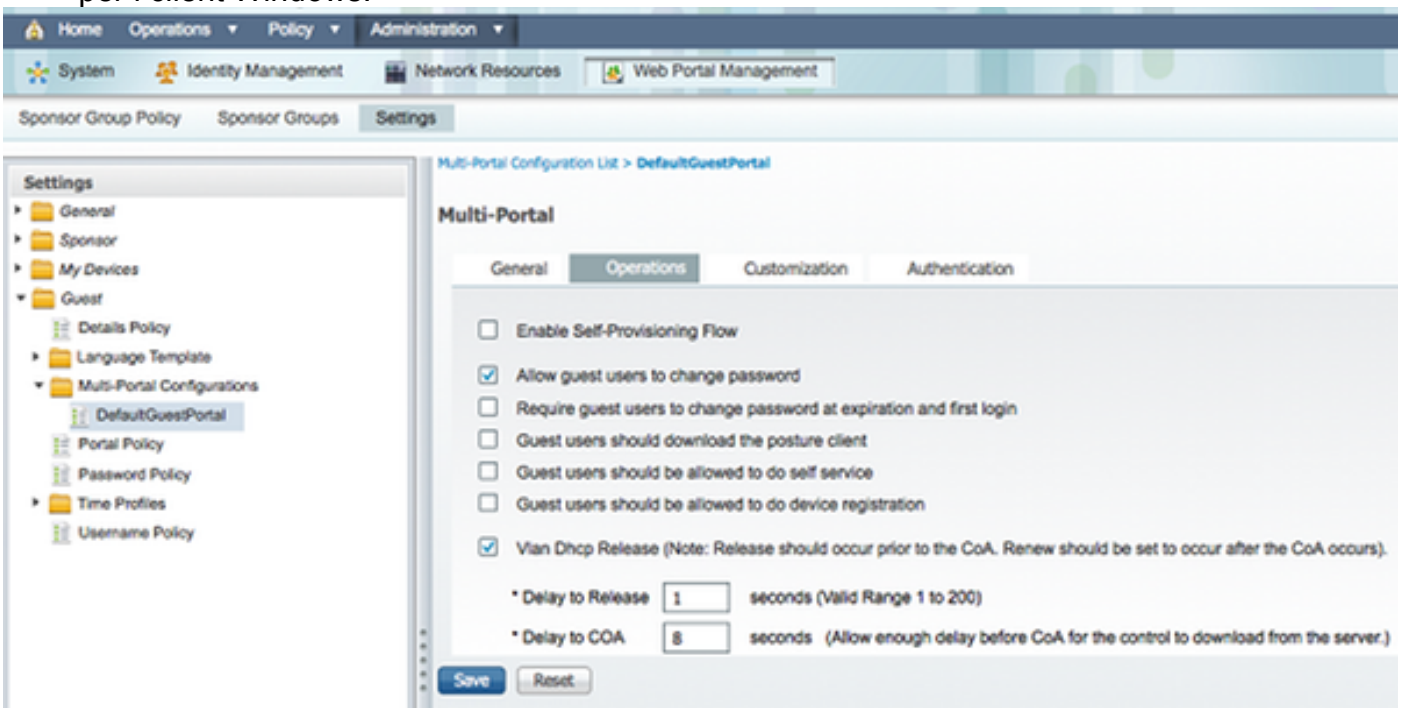
    È possibile scegliere l'opzione **Permit Access** (Autorizza accesso) o creare un profilo personalizzato in modo da restituire la VLAN o gli attributi desiderati.

Abilita rinnovo IP (facoltativo)

Se si assegna una VLAN, il passaggio finale è che il PC client rinnovi il proprio indirizzo IP. Questo passaggio viene eseguito dal portale guest per i client Windows. Se in precedenza non è stata impostata una VLAN per la *seconda* regola di *autenticazione*, è possibile ignorare questo passaggio.

Se è stata assegnata una VLAN, completare questi passaggi per abilitare il rinnovo dell'IP:

1. Fare clic su **Amministrazione** e quindi su **Gestione guest**.
2. Fare clic su **Impostazioni**.
3. Espandere **Guest** ed espandere **Configurazione portale multiplo**.
4. Fare clic su **DefaultGuestPortal** o sul nome di un portale personalizzato eventualmente creato.
5. Selezionare la casella di controllo **Vlan DHCP** Relase. **Nota:** Questa opzione funziona solo per i client Windows.



Configurazione switch (estratto)

In questa sezione viene fornito un estratto della configurazione dello switch. Per la configurazione completa, vedere Configurazione dello switch (completa).

In questo esempio viene illustrata una configurazione MAB semplice.

```
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
```

La VLAN 100 è la VLAN che fornisce la connettività di rete completa. Viene applicato un ACL della porta predefinita (denominato *webauth*) che viene definito come mostrato di seguito:

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

Questa configurazione di esempio fornisce l'accesso completo alla rete anche se l'utente non è autenticato; è pertanto consigliabile limitare l'accesso agli utenti non autenticati.

In questa configurazione, l'esplorazione HTTP e HTTPS non funziona senza autenticazione (secondo l'altro ACL) poiché ISE è configurato per utilizzare un ACL di reindirizzamento (denominato *reindirizzamento*). Di seguito è riportata la definizione sullo switch:

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

Questo elenco degli accessi deve essere definito sullo switch per definire il traffico su cui lo switch eseguirà il reindirizzamento. (Corrisponde al *permesso*.) In questo esempio, qualsiasi traffico HTTP o HTTPS inviato dal client attiva un reindirizzamento Web. Questo esempio nega anche l'indirizzo IP di ISE, in modo che il traffico diretto all'ISE venga indirizzato all'ISE e non venga reindirizzato in un loop. (in questo scenario, il comando deny non blocca il traffico; semplicemente non reindirizza il traffico). Se si utilizzano porte HTTP insolite o un proxy, è possibile aggiungere altre porte.

Un'altra possibilità consiste nel consentire l'accesso HTTP ad alcuni siti Web e il reindirizzamento ad altri. Ad esempio, se nell'ACL si definisce un'autorizzazione solo per i server Web interni, i client potrebbero navigare nel Web senza autenticarsi, ma potrebbero subire il reindirizzamento se tentano di accedere a un server Web interno.

L'ultimo passaggio consiste nel consentire l'accesso al CoA sullo switch. In caso contrario, ISE non potrà forzare lo switch a riautenticare il client.

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

Questo comando è necessario per il reindirizzamento dello switch in base al traffico HTTP:

```
ip http server
```

Questo comando è necessario per il reindirizzamento in base al traffico HTTPS:

```
ip http secure-server
```

Anche questi comandi sono importanti:

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

Se l'utente non è ancora autenticato, il comando **show authentication session int <interface num>** restituisce questo output:

```
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
```

Nota: Nonostante un'autenticazione MAB riuscita, l'ACL di reindirizzamento viene posizionato perché l'indirizzo MAC non era noto all'ISE.

Configurazione switch (completa)

In questa sezione viene elencata la configurazione completa dello switch. Alcune interfacce e righe di comando non necessarie sono state omesse; pertanto, questa configurazione di esempio deve essere utilizzata solo come riferimento e non deve essere copiata.

```
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
```

Configurazione proxy HTTP

Se si utilizza un proxy HTTP per i client, significa che i client:

- Usa una porta non convenzionale per il protocollo HTTP
- Invia tutto il traffico al proxy

Per fare in modo che lo switch ascolti la porta non convenzionale (ad esempio, 8080), utilizzare questi comandi:

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

Inoltre, è necessario configurare tutti i client in modo che continuino a utilizzare il proxy, ma non lo utilizzino per l'indirizzo IP di ISE. Tutti i browser includono una funzione che consente di immettere nomi host o indirizzi IP che non devono utilizzare il proxy. Se non si aggiunge l'eccezione per ISE, viene visualizzata una pagina di autenticazione loop.

Inoltre, è necessario modificare l'ACL di reindirizzamento in modo da consentire l'accesso alla porta proxy (nell'esempio riportato, 8080).

Nota importante sulle SVI degli switch

A questo punto, lo switch ha bisogno di un'interfaccia virtuale di switch (SVI) per rispondere al client e inviare il reindirizzamento del portale Web al client. Questa SVI non deve necessariamente trovarsi sulla subnet/VLAN del client. Tuttavia, se lo switch non ha SVI nella subnet/VLAN client, deve usare una delle altre SVI e inviare il traffico come definito nella tabella di routing del client. In genere, il traffico viene inviato a un altro gateway nel cuore della rete; il traffico torna allo switch di accesso all'interno della subnet del client.

I firewall in genere bloccano il traffico da e verso lo stesso switch, come in questo scenario, pertanto il reindirizzamento potrebbe non funzionare correttamente. Le soluzioni sono quelle di consentire questo comportamento sul firewall o di creare una SVI sullo switch di accesso nella subnet del client.

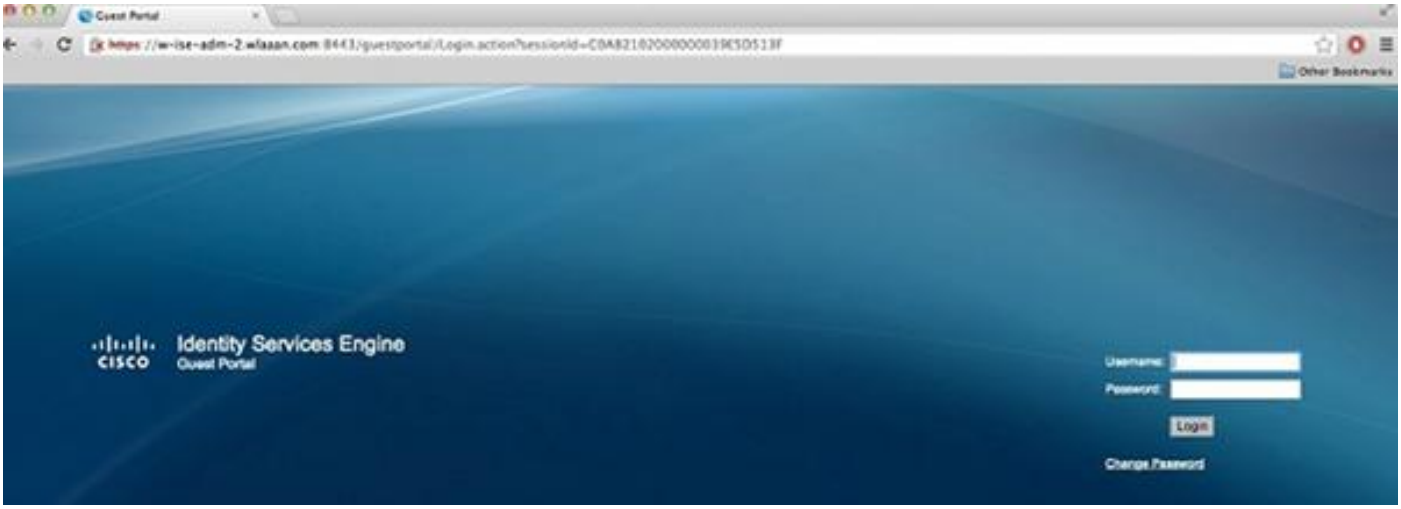
Nota importante sul reindirizzamento HTTPS

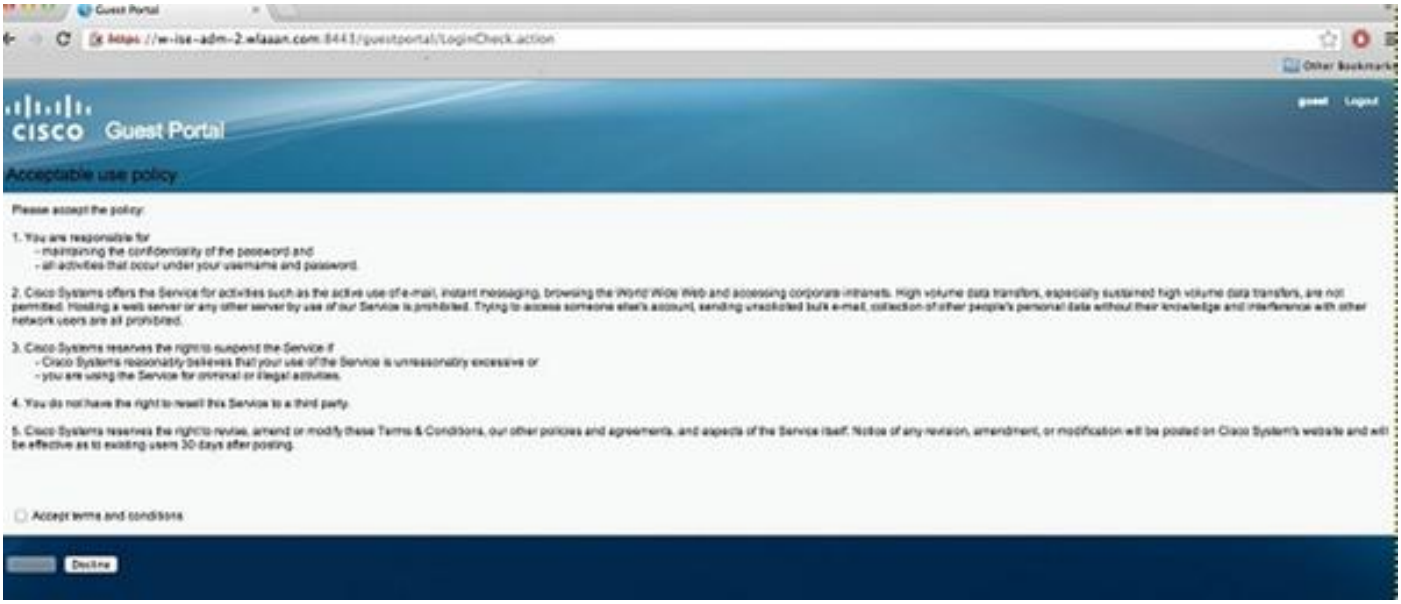
Gli switch possono reindirizzare il traffico HTTPS. Pertanto, se il client guest dispone di una home page in HTTPS, il reindirizzamento verrà eseguito correttamente.

L'intero concetto di reindirizzamento si basa sul fatto che un dispositivo (in questo caso lo switch) falsifica l'indirizzo IP del sito Web. Tuttavia, quando lo switch intercetta e reindirizza il traffico HTTPS, si verifica un problema grave perché lo switch può presentare solo il proprio certificato nell'handshake TLS (Transport Layer Security). Poiché non si tratta dello stesso certificato del sito Web richiesto in origine, la maggior parte dei browser emette avvisi principali. I browser gestiscono correttamente il reindirizzamento e la presentazione di un altro certificato come un problema di protezione. Non sono disponibili soluzioni alternative e lo switch non può falsificare il certificato originale del sito Web.

Risultato finale

Il PC client si collega ed esegue il MAB. Poiché l'indirizzo MAC non è noto, ISE rimanda indietro gli attributi di reindirizzamento allo switch. L'utente tenta di accedere a un sito Web e viene reindirizzato.





Quando l'autenticazione della pagina di login ha esito positivo, ISE rimbalza sulla porta dello switch tramite Change Of Authorization, che avvia di nuovo un'autenticazione MAB di layer 2.

Tuttavia, ISE sa che si tratta di un precedente client webauth e autorizza il client in base alle credenziali webauth (anche se si tratta di un'autenticazione di layer 2).

Nei log di autenticazione ISE, l'autenticazione MAB viene visualizzata in fondo al log. Sebbene

non sia noto, l'indirizzo MAC è stato autenticato e profilato e sono stati restituiti gli attributi webauth. Successivamente, l'autenticazione viene eseguita con il nome utente dell'utente, ovvero l'utente digita le proprie credenziali nella pagina Accesso. Subito dopo l'autenticazione, viene eseguita una nuova autenticazione di layer 2 con il nome utente come credenziali; in questo passaggio di autenticazione è possibile restituire attributi, ad esempio VLAN dinamica.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Cisco Identity Services Engine
- Guida di riferimento ai comandi di Cisco Identity Services Engine
- Integrazione di ISE (Identity Services Engine) con Cisco WLC (Wireless LAN Controller)
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems