

FORMAÇÃO EM CIBERSEGURANÇA

CISCO ISE - DEMO LAB
(AUTH MAB, 802.1X E ACTIVE
DIRECTORY)

CIBERSEGURANCA.CISCO.COM.BR

JANEIRO/2025

DISCLAIMER

Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

A configuração mostrada não é uma recomendação. O autor não se responsabiliza por má utilização do material, que tem objetivo exclusivamente educativo (use-o para testar e aprender a ferramenta).

Esse ebook foi constituído a partir de artigos publicados de 2019 a 2021 no blog da TechRebels no medium.com pelo mesmo autor.

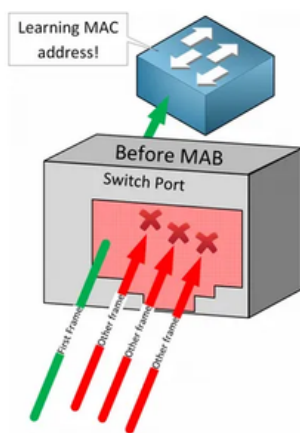
A versão utilizada do Cisco ISE na época era a 2.1, mas o conceito, telas e configuração continuam válidas para as versões atuais 3.x.

INTRODUÇÃO

Após conhecermos um pouco do ISE e fazermos um tour pelas principais funcionalidades no ebook anterior, vamos agora logo para o que interessa! Faremos duas configurações de autenticação básicas de MAB e 802.1x.

Primeiro as definições:

- MAB que é o acrônimo de *Mac Authentication Bypass*: é um mecanismo que permite a integração de equipamentos que não suportam 802.1x se autenticarem na rede.

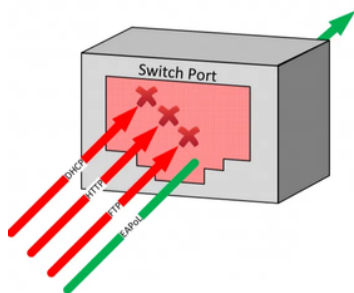


Quando habilitamos o MAB numa porta do switch, essa porta libera apenas o primeiro pacote (para aprender o endereço MAC), ficando todos os outros bloqueados até que a autenticação ocorra.

Ele não é um mecanismo muito seguro, já que é fácil spoofar um MAC, portanto, muitas vezes é utilizado como fallback do 802.1x.

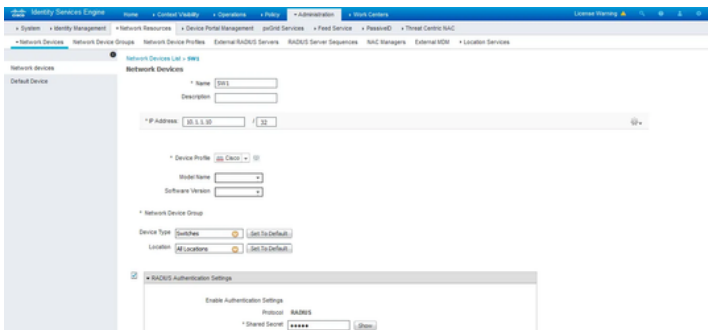
- 802.1x, às vezes chamado de Dot1x, é um protocolo padrão IEEE para controle de acesso à rede. Ele faz parte do grupo IEEE 802.1 de protocolos de redes de computadores. A IEEE 802.1x define o encapsulamento do Extensible Authentication Protocol (EAP) sobre IEEE 802, que é conhecido como “EAP over LAN” ou EAPOL. Isso significa que qualquer computador que tentar se conectar à rede, deverá primeiro fornecer informações de autenticação.

Before 802.1X Authentication



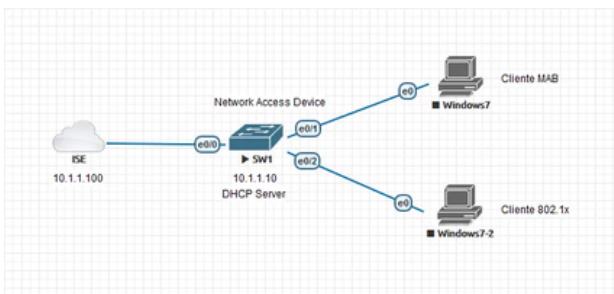
CONFIGURAÇÃO

Relembrando, no primeiro ebook, nós fizemos a configuração do switch no ISE.



A única diferença, é que eu criei um grupo para nosso **NAD** (apenas para organização), chamado Switches, repare na figura acima.

A topologia do nosso lab ficou assim (adicionei mais um cliente para o 802.1x):



Acessando o switch, veja as configurações simples de IP e teste básico de conectividade.



4) Vamos habilitar a autenticação, autorização e accounting via Dot1x e MAB – sempre apontando para o grupo ‘ISE’ que criamos no passo 2

```
❏ aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
```

5) Habilitar o ip device tracking e o Dot1x no switch

```
❏ ip device tracking
dot1x system-auth
```

6) Agora faremos configuração da porta e0/1, onde está o cliente MAB

```
❏ interface ethernet0/1
switchport mode access
dot1x pae authenticator
mab
authentication order mab dot1x
authentication priority dot1x mab
authentication port-control auto
```



7) E finalmente a configuração da porta e0/2, onde está o cliente Dot1x (idem acima, pois ambas estão habilitadas MAB e Dot1x)

```
interface ethernet0/2
  switchport mode access
  dot1x pae authenticator
  mab
  authentication order mab dot1x
  authentication priority dot1x mab
  authentication port-control auto
```

Como última task, vamos rapidinho criar um DHCP Server no switch:

```
ip dhcp excluded-address 10.1.1.1
!IP do meu notebook
ip dhcp excluded-address 10.1.1.10
!IP do switch
ip dhcp excluded-address 10.1.1.100
!IP do ISE

ip dhcp pool VLAN1
  network 10.1.1.0 /24
  default-router 10.1.1.10
  dns-server 10.1.1.10
```



Nesse momento, eu costumo fazer um teste simples de autenticação, veja abaixo:



```
SW1#test aaa group ISE fernando
Cisco123! legacy
```

```
Attempting authentication test to
server-group ISE using radius
User was successfully authenticated.
```

Esse usuário fernando, nós criamos no ebook anterior.

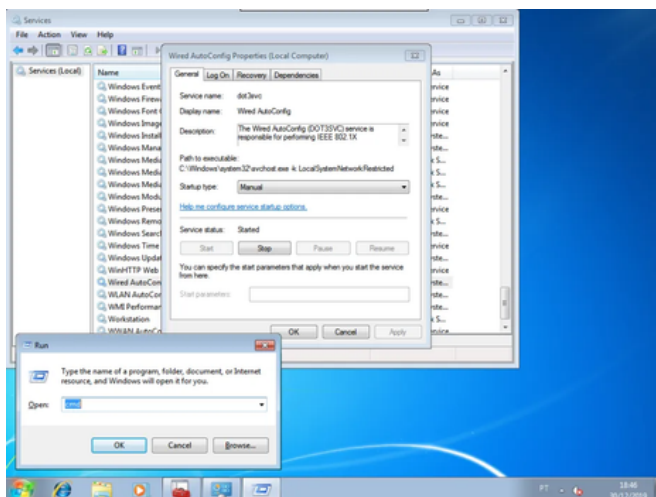
Aqui, os logs do ISE em *Operations > RADIUS > Live Logs*:

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint	Authentica.	Authorizati.	Authorizati.	IP Address	Network Device
Dec 30, 2019 10:23:54 AM	Success			fernando	Endpoint ID	Endpoint IP	Default = S	Default = S	Permissions		SW1

Começando então pelo cliente do 802.1X, já que o usuário já está criado e OK.

Acessando a máquina Windows, vamos confirmar que o serviço *WiredAutoConfig*, que habilita o 802.1X na LAN está rodando. Em caso negativo, inicie ele:

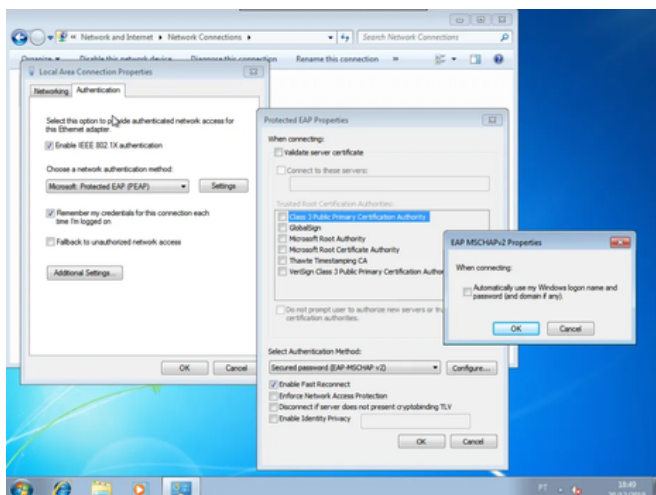




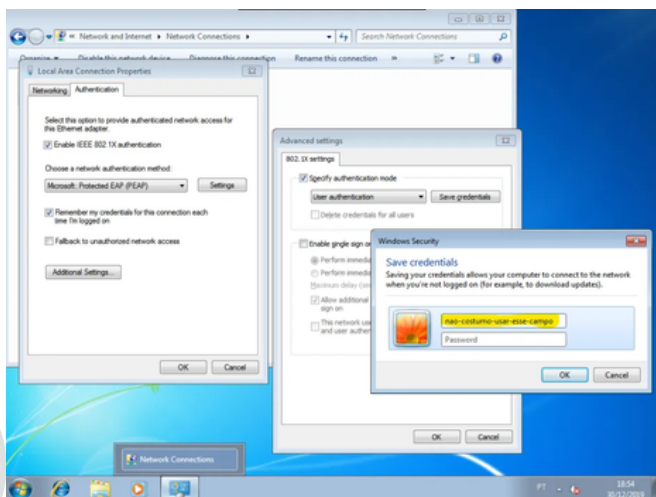
Agora a configuração da placa de rede. Clicar com o botão direito, propriedades e aba Authentication:

Selecione PEAP e depois em configurações, desmarque para validar o certificado do servidor (já que não estamos usando certificado digital nesse caso) e, em configuração do método de autenticação, desmarque para usarmos o usuário do Windows.

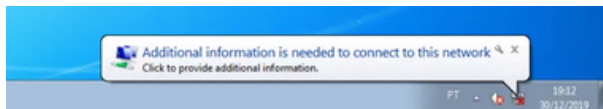




Dê OK em tudo e em configurações adicionais, deixe marcado para autenticação de usuário – aqui eu costumo deixar sem user e password pré-definidos, mas você pode configurar se preferir.



E, finalmente, estamos prontos para o teste. A porta do switch estava em shutdown, alterei ela, e apareceu um balão no Windows pedindo usuário e senha (caso não aconteça, desabilite e habilite o adaptador de rede):




Clique nele e entre com usuário fernando, que criamos no post anterior e testamos no switch no início do artigo.

Repare agora nas telas que confirmam a autenticação bem sucedida.

Logs do ISE em *Operations > RADIUS > Live Logs*

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint	Authenticat	Authorizati	Authorizati	IP Address	Network Device
Dec 30, 2019 04:10:30.725 PM	Success		0	fernando	00:00:00:00:00	Windows/...	Default => S...	Default => S...	PermitAccess	10.1.1.2	Network Device
Dec 30, 2019 04:10:30.453 PM	Success		0	fernando	00:00:00:00:00	Unknown	Default => S...	Default => S...	PermitAccess		Switch

 **Obs:** São duas entradas pois a de baixo é a autenticação em si, e a de cima, a sessão RADIUS que foi criada.

E nosso cliente se autenticou e já pegou IP:



```

C:\Windows\system32\cmd.exe
Mode Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter Local Area Connection1:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) PRO/1000 MT Network Connection
Physical Address. . . . . : 50-00-00-03-00-00
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80:16c43:ad84:955:6d72:x11(Preferred)
IPv4 Address. . . . . : 10.1.1.2(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : segunda-feira, 30 de dezembro de 2019 10:19:24
Lease Expires . . . . . : terça-feira, 31 de dezembro de 2019 10:19:24

Default Gateway . . . . . : 10.1.1.10
DHCP Server . . . . . : 10.1.1.10
DHCPv6 IIF . . . . . : 240123904
DHCPv6 Client DUID. . . . . : 00-01-00-01-23-4F-26-33-50-00-00-01-00-00-00


DNS Suffix . . . . . : 10.1.1.0
NetBIOS over Tcpip. . . . . : Enabled

Tunnel adapter Isatap.{CEF0D1B7-C27F-42B2-9795-EF0F576D010F}:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . : 
Description . . . . . : Microsoft ISATAP Adapter
Physical Address. . . . . : 00-00-00-00-00-00-E0
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes

C:\Users\Fernando>

```

 Dê um *'show authentication sessions'* no switch e você verá a autenticação e autorização bem sucedida. Repare no método:

```

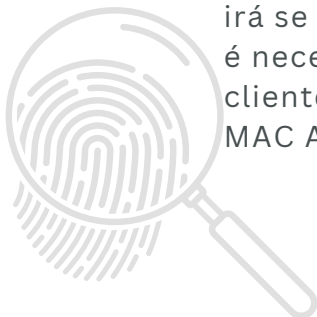
SW1#sh auth sessions
Interface Identifier Method Domain Status Fg Session ID
Et0/2 5000.0003.0000 dot1x DATA Auth
0A01010A00000013004B82AB

Session count = 1

Key to Session Events Blocked Status Flags:
A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker

```

Vamos agora ligar a máquina Windows que irá se autenticar com MAB. Nesse caso, não é necessário nenhuma configuração no cliente. Nos logs do ISE, agora vemos um MAC Address ao invés de um usuário.



Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint	Authenticat.	Authorizati.	Authorizati.	IP Address	Network Device
Dec 30, 2019 04:38:40:323 PM	●		1	Identity	5000.0002.0000	10.00.00.02.00.00	MabAuth	Default vs R	Default vs R	PermisAccess	10.1.1.3
Dec 30, 2019 04:34:20:901 PM	■				5000.0003.0000	10.00.00.02.00.00	Unknown	Default vs R	Default vs R	PermisAccess	10.1.1.3

No switch, temos agora duas portas autenticadas. A primeira é a do MAB e a segunda do 802.1X. Repare no método em destaque:

```
SW1#show authentication sessions

Interface  Identifier  Method  Domain  Status Fg Session ID
Et0/1     5000.0002.0000  mab     DATA   Auth
0A01010A0000001400585EC1
Et0/2     5000.0003.0000  dot1x   DATA   Auth
0A01010A00000013004B82AB

Session count = 2

Key to Session Events Blocked Status Flags:

A - Applying Policy (multi-line status for details)
D - Awaiting Deletion
F - Final Removal in progress
I - Awaiting IIF ID allocation
N - Waiting for AAA to come up
P - Pushed Session
R - Removing User Profile (multi-line status for details)
U - Applying User Profile (multi-line status for details)
X - Unknown Blocker
```


O Windows também pegou um IP, assim como a primeira máquina:

```
SW1#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address      Client-ID/      Lease expiration        Type
State           Interface
                Hardware address/
                User name
10.1.1.2        0150.0000.0300.00    Dec 31 2019 08:19 PM
Automatic      Active           Vlan1
10.1.1.3        0150.0000.0200.00    Dec 31 2019 08:38 PM
Automatic      Active           Vlan1
```

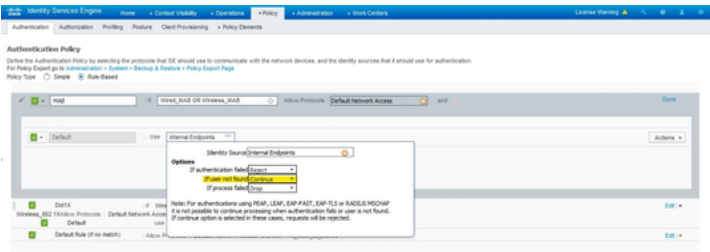


E, por fim, tráfego liberado entre as máquinas.

```
SW1#ping 10.1.1.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.2, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms
SW1#ping 10.1.1.3
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.1.3, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
```

 **Obs:** Você deve ter reparado que no caso do cliente Dot1x nós criamos um usuário, mas não criamos um **endpoint** para o cliente MAB. Isso porque por padrão na versão 2.1, o ISE mesmo que não exista um endpoint, ele permite que o processo continue.

Essa configuração é feita aqui:



The screenshot shows the Cisco ISE Administration console for the Authentication Policy configuration. The 'Options' section is expanded, showing the following settings:

- Authentication Fail: Continue
- Failure Not Found: Continue

A tooltip is visible over the 'Failure Not Found' dropdown, containing the text: "Notes: For authentications using RADIUS, LDAP, S80, EAP, etc., if a user is not found, it is not possible to continue processing when Authentication fails or user is not found. If continue option is selected in these cases, requests will be rejected."



ACTIVE DIRECTORY

A configuração é extremamente simples, mas 3 pré-requisitos importantes podem nos fazer perder um bom tempo no troubleshooting:

- horário sincronizado (seja usando NTP – recomendado – ou manualmente);
- mesmo timezone;
- ISE apontando o DNS pro AD – ou um dos ADs do domínio.

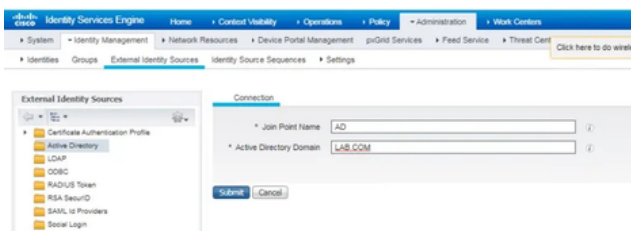
Fora isso, você precisará de um usuário com permissão para criar um objeto no AD (meus tempos de MCSE já passaram então não lembro se é necessário esse usuário fazer parte do grupo Domain Admins, ou se tem algum outro grupo mais restritivo que permita a criação desse objeto).

Tendo isso em mãos, vamos pro ISE – aqui, consegui atualizar meu lab e estou usando a versão 2.7, atualmente recomendada pela Cisco.

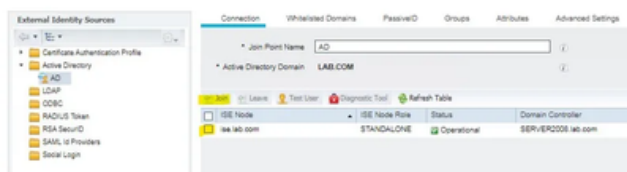
Vamos então configurar o AD, que é uma base externa de usuários, ok?

Menu Administration > External Identity Source > Active Directory

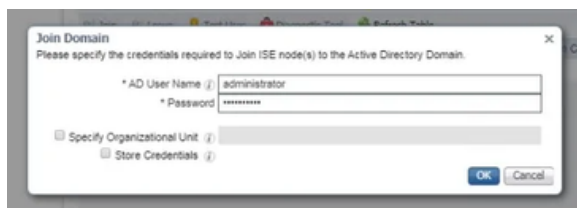




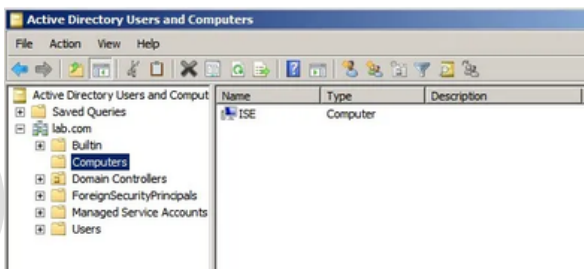
O *Join Point Name* é apenas um nome que você vai dar para essa base de usuários e o AD Domain o seu domínio.



Depois do Submit, marque a caixa de seleção ao lado e clique em Join. Entre com usuário e senha conforme falamos acima:



Você receberá uma mensagem de sucesso (se não, verifique os pré-reqs acima) e o objeto do ISE será criado no seu AD:



CUSTOMIZAÇÃO

Vamos agora customizar as políticas de autenticação e autorização.

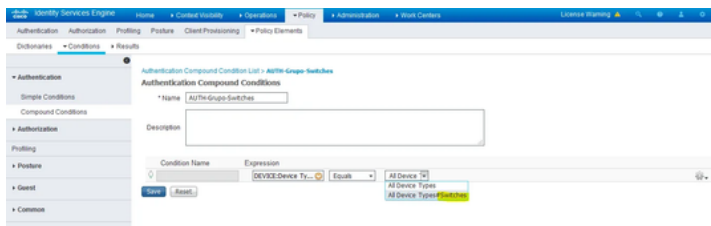
A intenção é que você perceba a granularidade do ISE.

Nosso objetivo: Vamos negar a regra padrão de autenticação e não vamos mexer na regra de MAB. Mas, para 802.1X, vamos autenticar apenas os switches dentro do grupo “Switches” e os usuários criados localmente no ISE que fazem parte do grupo Lab_Admin. Por fim, para essa mesma regra, vamos aplicar uma VLAN e uma DACL (Downloadable ACL) caso a autenticação seja bem sucedida.

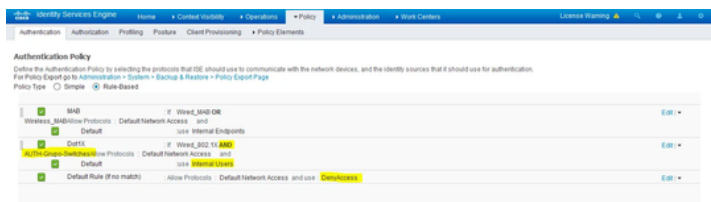
Lembrando que esse artigo é uma continuação dos anteriores, caso você não entenda algo, consulte eles, ok?

Vamos começar clicando em *Policy > Conditions > Authentication e Compound Conditions*. Aqui, vamos criar uma nova condição para que uma autenticação ocorra. Nela vamos selecionar apenas o grupo “Switches” que criamos nos artigos anteriores, que é onde colocamos o nosso switch de teste “SW1”.

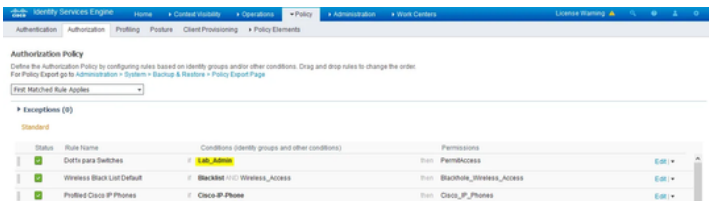




Agora aplicamos essa nova condição. Vá para *Policy > Authentication*, negue a última regra padrão (isso só para essa versão que estamos usando, a 2.1) e edite a regra de Dot1x. Na condição, remova *Wireless_802.1x*, altere a regra para **AND**, e selecione a condição que criamos acima. Por fim, na última caixa, altere qual base de dados o ISE irá pesquisar. Altere de *All_User_ID_Stores* para *Internal Users*. Ou seja, apenas usuários criados localmente poderão se autenticar. Caso houvesse uma base do AD integrada (futuramente faremos isso), esses usuários externos não poderiam se autenticar. Por fim, salve tudo.

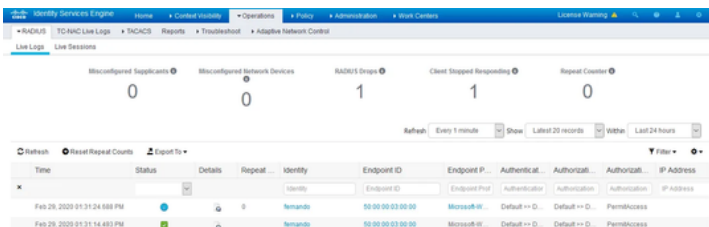


Vamos agora para *Policy > Authorization* e crie uma nova regra. Nomeie como está abaixo e edite a condição. Selecione dentro de *User Identities Store*, o grupo **Lab_Admin**. É nesse grupo que nosso usuário de teste “Fernando” está inserido (também foi criado nos artigos anteriores).



Status	Rule Name	Conditions (Identify groups and other conditions)	Permissions
On	Defin para Switches	Lab_Admin	PermAccess
On	Wireless Black List Default	Blacklist >>> Wireless_Access	Blocklist_Wireless_Access
On	Proteged Cisco IP Phones	Cisco-IP-Phone	Cisco_IP_Phones

Ligue a VM do Windows e vamos testar a autenticação, que ocorrerá com sucesso. Veja abaixo em *Operations > Radius > Live Logs*.



Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...	Authenticat...	Authorizati...	Authorizati...	IP Address
Feb 28, 2020 01:31:24:688 PM	Success		0	Fernando	50:00:00:00:00:00	Microsoft-...	Default == D...	Default == D...	PermAccess	
Feb 28, 2020 01:31:14:493 PM	Success		0	Fernando	50:00:00:00:00:00	Microsoft-...	Default == D...	Default == D...	PermAccess	

Caso tentemos autenticar um usuário “Henrique” que eu criei agora, mas não faz parte do grupo Lab_Admin, veja o resultado:



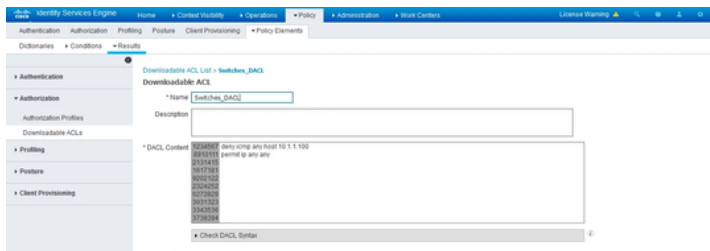
Identity Services Engine		Steps
Overview Event: 5409 Authentication failed Username: henrique Endpoint Id: 50.00.00.03.00.00 ID Endpoint Profile: Microsoft/Workstation Authentication Policy: Default vs Deltix vs Default ✓ Authorization Policy: Default vs Basic Authentication Access Authorization Result: Unauthorized		11001 Received RADIUS Access-Request 11017 RADIUS created a new session 15048 Evaluating Policy Group 15048 Evaluating Service Selection Policy 15048 Queried PP - Normalized Radius Radius/reqType 15048 Queried PP - DEVICE Device Type 15044 Matched rule - Deltix 11007 Extracted EAP-Response/Identity 12003 Prepared EAP-Request proposing EAP-TLS with challenge 12005 Valid EAP-Request/req-type attribute received 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12001 Extracted EAP-Response/TXK requesting to use PEAP instead 12000 Prepared EAP-Request proposing PEAP with challenge 12005 Valid EAP-Request/req-type attribute received 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12002 Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as requested 12010 Successfully negotiated PEAP version 0 12000 Extracted first TLS record; TLS handshake started 12005 Extracted TLS ClientHello message 12006 Prepared TLS ServerHello message 12007 Prepared TLS Certificate message 12008 Prepared TLS ServerKeyExchange message
Authentication Details Source Timestamp: 2020-02-29 18:06:52:165 Received Timestamp: 2020-02-29 18:06:52:213 Policy Served: on Event: 5409 Authentication failed Failure Reason: 11018 Requested per authentication profile Resolution: Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule results. Root cause: Selected Authorization Profile contains ACCESS_REJECT attribute Username: henrique		

O processo de autenticação passou, pois a condição para o switch está OK, mas o usuário não obteve autorização para o login. O processo deu match na nossa regra de autenticação mas, na autorização, ele bateu na regra default, que **nega o acesso**. Analise a figura pra entender bem. A quantidade de informação é grande, e isso facilita muito o *troubleshooting*.

Cavando um pouquinho mais, vamos agora ao invés de **apenas permitir o acesso**, vamos criar um profile e **aplicar configurações no switch**, caso a autenticação seja bem sucedida.

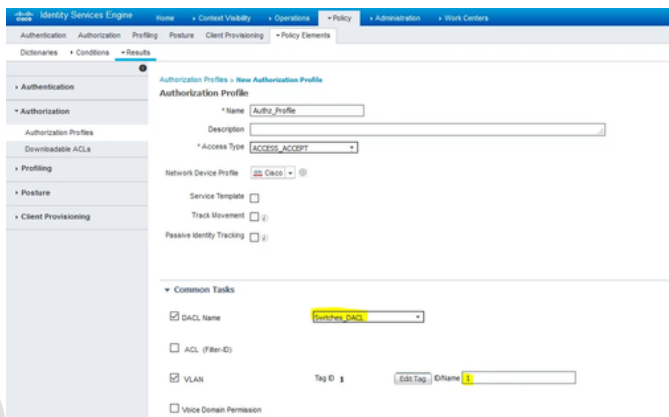
Clique em *Policy > Policy Elements > Results > Authorization > Downloadable ACLs*. Conforme a figura, vamos criar uma ACL que será enviada pelo ISE para o switch especificamente para esse usuário nessa porta que ele se autenticou.





A granularidade aqui é de uma ACL comum ok? No nosso exemplo, vamos apenas negar o ping para o ISE. De resto, tudo permanece liberado.

Agora, ainda nesse menu, vá no item acima e à esquerda: *Authorization Profiles*. Acompanhe na figura, você irá escolher a DACL que criamos e também irá setar uma VLAN específica para esse usuário. No nosso caso será a **VLAN 1** mesmo, já que não criamos outra.



E aí ficou fácil! Vamos voltar pra Autenticação e Autorização e, ao invés de selecionar “*PermitAccess*”, vamos escolher esse *Authorization Profile* que acabamos de criar. Veja, como ficou:

Status	Rule Name	Conditions (Identify groups and other conditions)	Permissions
On	Lab para Switches	Lab	Authn_Profile
On	Wireless Back List Default	Backend	Backend_Wireless_Access
On	Profiled Cisco IP Phones	Cisco_IP_Phone	Cisco_IP_Phone
On	Profiled Non Cisco IP Phones	Non_Cisco_Profiled_Phones	Non_Cisco_IP_Phone

Vamos testar novamente a autenticação. Dê um *bounce* na placa de rede, e um *clear authentication sessions* no switch. Entre com o usuário “Fernando” na caixa que vai aparecer no Windows e analise os logs:

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint IP	Authenticat...	Authorizati...	Authorizati...	IP Address	Network Device
Feb 20, 2020 01:45:51:363 PM	Success		0	fernando	00 00 00 00 00	10.1.1.2	Default => S...	Default => S...	Authn_Profile	10.1.1.2	SW1
Feb 20, 2020 01:45:13:437 PM	Success		0	fernando	00 00 00 00 00	10.1.1.2	Default => S...	Default => S...	Authn_Profile	10.1.1.2	SW1

Repare acima que a ACL foi enviada com sucesso para o switch.

Abrindo o log da ACL (na lupinha em *Details*), veja a mensagem de sucesso e o nosso network device “SW1”.



Identity Services Engine		Steps
Overview		
Event	5232 DACL Download Succeeded	11001 Received RADIUS Access-Request
Username	#ACSACLx-IP-Switches_DACL-5e5a93c0	11017 RADIUS created a new session
Endpoint ID		11117 Generated a new session ID for a 3rd party NAD
Endpoint Profile		11002 Returned RADIUS Access-Accept
Authorization Result		
Authentication Details		
Source Timestamp	2025-02-29 13:45:13.327	
Received Timestamp	2025-02-29 13:45:13.487	
Policy Server	ise	
Event	5232 DACL Download Succeeded	
Username	#ACSACLx-IP-Switches_DACL-5e5a93c0	
Network Device	SW1	
Device Type	All Device Types@Switches	
Location	All Locations	
NAS IPv4 Address	10.1.1.10	
Response Time	01	

No switch, entre com o comando *show authentication sessions int e0/2 details* e você terá o seguinte:

```
SW1#show auth sessions int e0/2 details
  Interface: Ethernet0/2
  MAC Address: 5000.0003.0000
  IPv6 Address: Unknown
  IPv4 Address: 10.1.1.2
  User-Name: fernando
  Status: Authorized
  Domain: DATA
  Oper host mode: single-host
  Oper control dir: both
  Session timeout: N/A
  Restart timeout: N/A
  Periodic Acct timeout: N/A
  Session Uptime: 49s
  Common Session ID: 0A01010A00000000E000E343B
  Acct Session ID: 0x00000004
  Handle: 0xA9000002
  Current Policy: POLICY_Et0/2

Local Policies:
  Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE
(priority 150)
  Security Policy: Should Secure
  Security Status: Link Unsecure

Server Policies:
  Vlan Group: Vlan: 1
  ACS ACL: xACSACLx-IP-Switches_DACL-5e5a93c0

Method status list:
  Method          State
  mab              Stopped
  dot1x           Authc Success
```

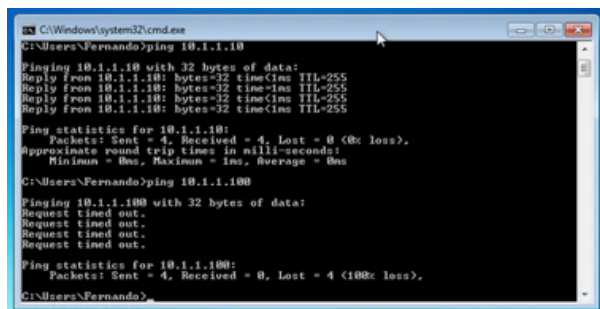


Repare na sessão “*Server Policies*” destacada. Você verá que foi aplicada a vlan 1 e a ACL que criamos nessa interface eth0/2 apenas.

Para complementar, veja também o *show ip access-list*.

```
SW1#show ip access-list
Extended IP access list xACSACLx-IP-Switches_DACL-5e5a93c0 (per-user)
 1 deny icmp any host 10.1.1.100
 2 permit ip any any
```

Finalizando, vá para a máquina Windows e tente pingar o IP 10.1.1.100 e também o 10.1.1.10 (que é o SW1) ;D



```
C:\Windows\system32\cmd.exe
C:\Users\Fernando>ping 10.1.1.10

Pinging 10.1.1.10 with 32 bytes of data:
Reply from 10.1.1.10: bytes=32 time<ms TTL=255
Reply from 10.1.1.10: bytes=32 time<ms TTL=255
Reply from 10.1.1.10: bytes=32 time<ms TTL=255
Reply from 10.1.1.10: bytes=32 time<ms TTL=255

Ping statistics for 10.1.1.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Fernando>ping 10.1.1.100

Pinging 10.1.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 10.1.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Users\Fernando>
```



AGRADECIMENTOS

Gostaria de agradecer a todos os leitores e seguidores do blog TechRebels nesses anos todos. Foi sensacional ter tido a chance de conhecer alguns pessoalmente.

Espero que o conteúdo possa ajudar muito mais pessoas a aprender sobre essa solução que continua dominando o mercado e não para de crescer em funcionalidades e adoção!

Se você recebeu esse ebook de um amigo, dê uma olhada nos treinamentos que temos disponíveis no ciberseguranca.cisco.com.br.

Grande abraço e muito sucesso!!!



[linkedin.com/in/fmp7/](https://www.linkedin.com/in/fmp7/)

