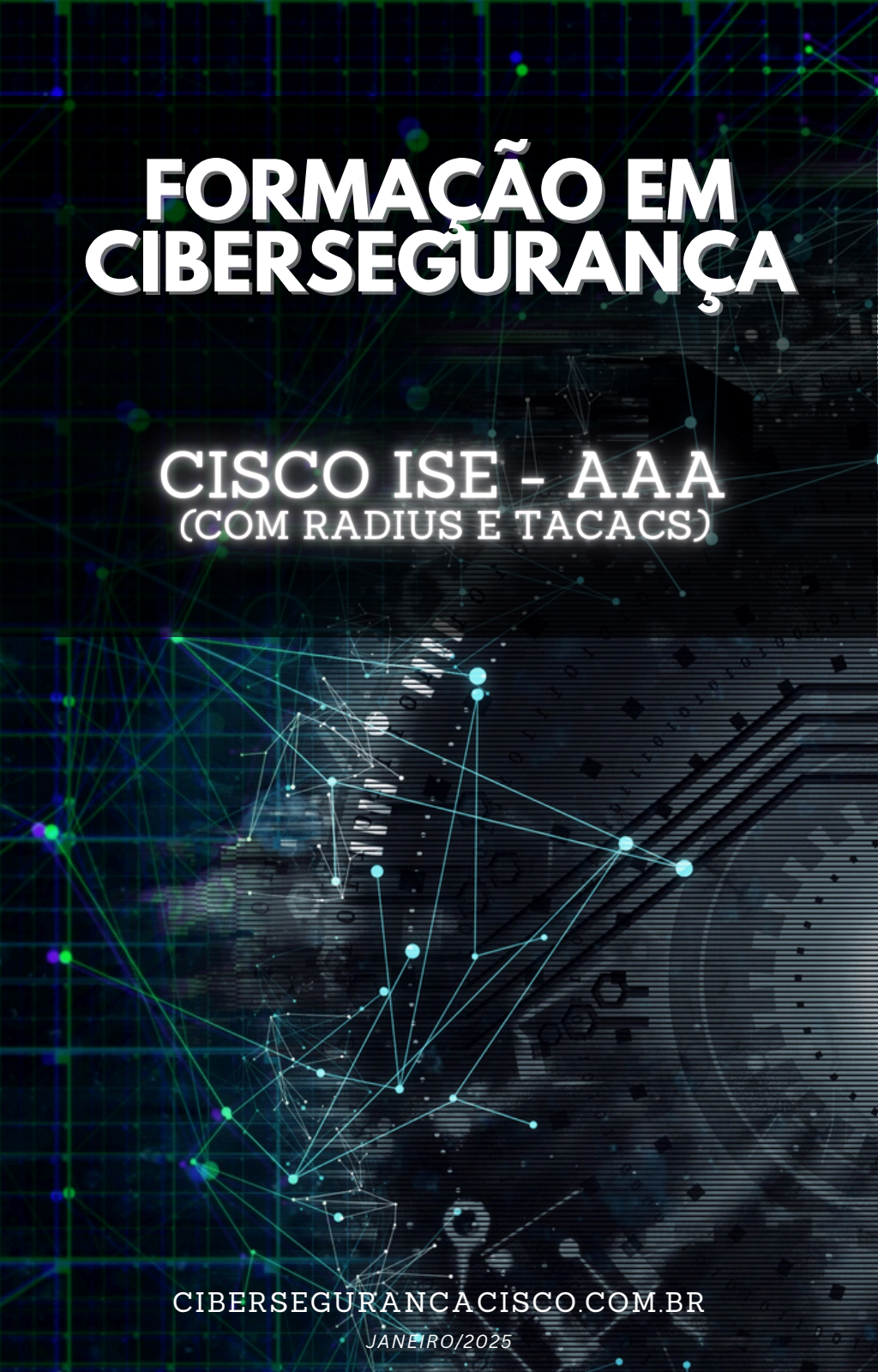
FORMAÇÃO EM CIBERSEGURANÇA

CISCO ISE - AAA
(COM RADIUS E TACACS)



CIBERSEGURANCACISCO.COM.BR

JANEIRO/2025

DISCLAIMER

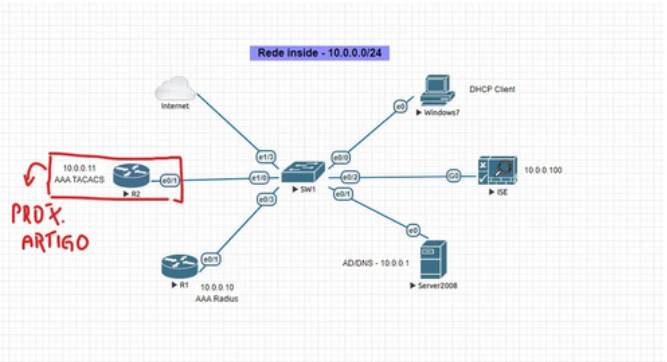
Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

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.

RADIUS



Vamos falar sobre um dos meus assuntos preferidos hoje: **AAA (Authentication, Authorization e Accounting)!**

Nosso objetivo é logar em um router via SSH, com um usuário do AD autenticando no ISE e obter privilégio 15 automaticamente.

Relembrando:
O ebook anterior mostra o processo de configurar o NAD (Router, Switch, etc.) no ISE e como fazer a integração entre o AD e o ISE.

Bom, nesse momento, temos nosso router configurado (servidor Radius) e o AD integrado ao ISE. Repare na topologia acima. Estamos configurando o R1.
Vamos aplicar as configurações de AAA no roteador:

```
aaa authentication login SEMAUTENTIC
none
aaa authentication login ISE group ISE
aaa authorization exec ISE group ISE
```

O primeiro comando, cria um grupo de autenticação “sem autenticação”. SEMAUTENTIC é o nome que eu dei e associei a um método ‘none’. Vamos configurar esse método na line con do router, para não ficarmos presos “pra fora” do roteador caso algo dê errado.

O segundo comando cria um grupo de autenticação “ISE” e associa ao grupo “ISE”, que é o nome do servidor que eu criei no artigo com o link acima. Os nomes iguais foram preferência minha, ok? Eles não precisam ser iguais.

Agora que já sabemos “quem” é a pessoa que vai logar no router, veremos “o que” ela pode fazer. Essa parte é bem simples e menos granular do que usando o protocolo TACACS.

Nós já definimos os métodos de autenticação e autorização e apontamos eles para o grupo de servidores Radius chamado ISE. Agora, vamos linkar esses métodos no acesso aos eqtos.

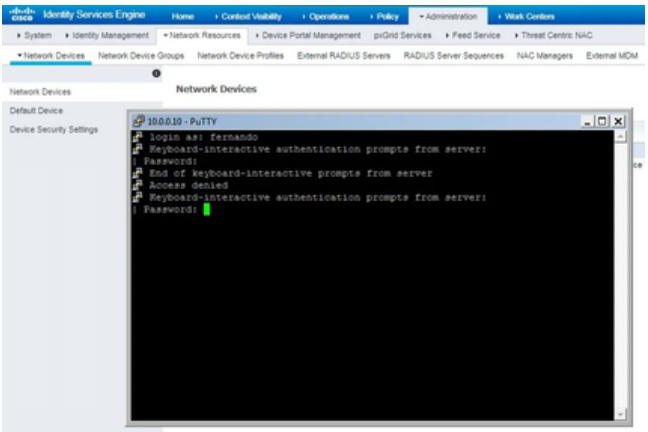
```
line con 0
 logging synchronous
 login authentication SEMAUTENTIC

line vty 0 4
 authorization exec ISE
 login authentication ISE
 transport input ssh
```

Repare na line vty que estou usando SSH. Portanto, não esqueça de gerar a chave rsa com o comando:

```
crypto key generate rsa label MINHA-CHAVE modulus 2048
```

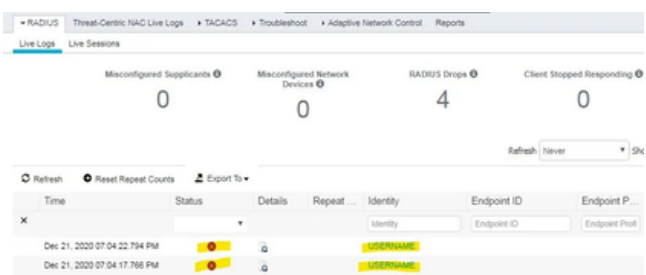
Finalizamos a parte do router.

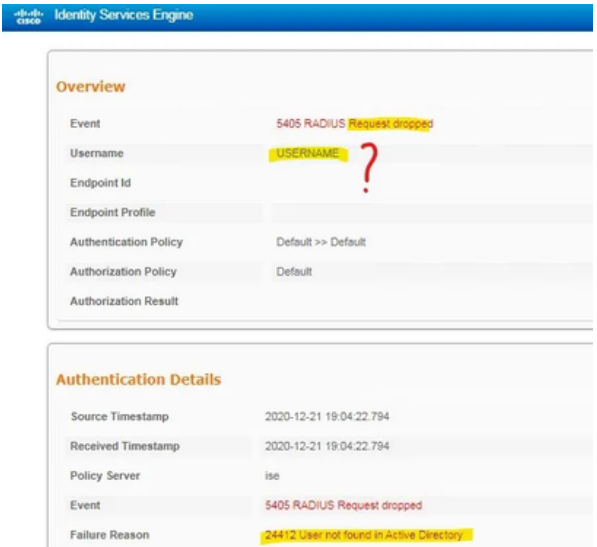
Vamos fazer um teste de autenticação agora sem nenhuma configuração adicional no ISE. Veja o resultado:



Olhando os logs do ISE:

Obs: Pessoal, não vou ficar repetindo os menus ou como encontrar a informação na GUI do ISE. Está tudo explicado nos outros ebooks, ok?



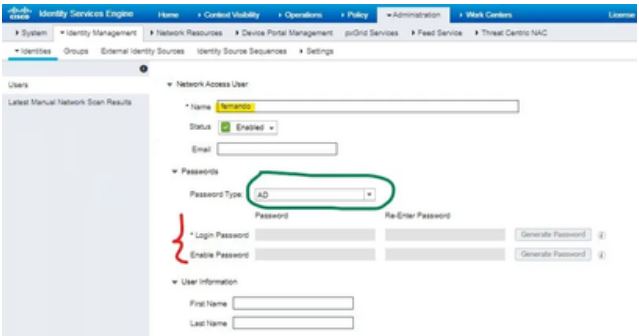


O padrão do ISE, é procurar em todas as bases de usuários configuradas. Portanto, ele procurou no AD, mas não encontrou meu usuário 'fernando'.

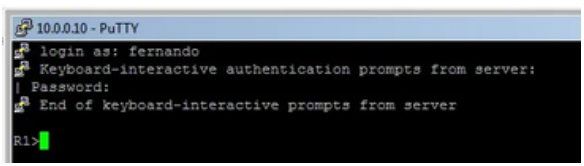
Vou então criá-lo agora no AD (feito!) e também dentro do ISE, mas apontando a senha para o 'AD'. Isso me permitirá adicionar esse user dentro de um grupo do próprio ISE.

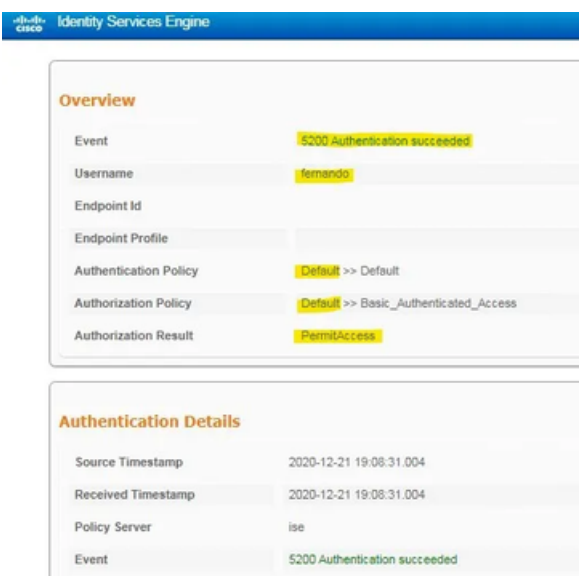
Obs: Tem inúmeras formas de fazer essas associações, seja por grupo no AD, no ISE, etc...

Reparem no "Password Type":



Fazemos outro teste de autenticação agora e vejam o resultado:

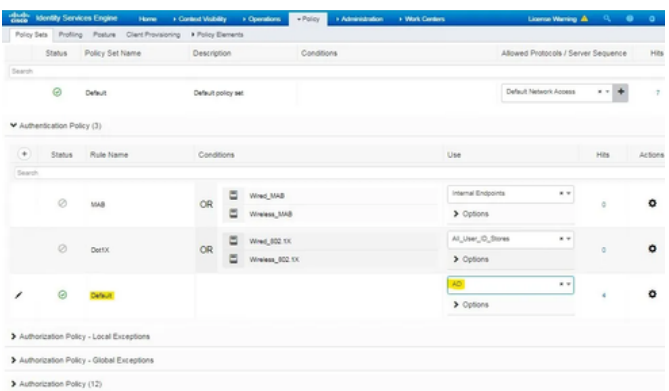




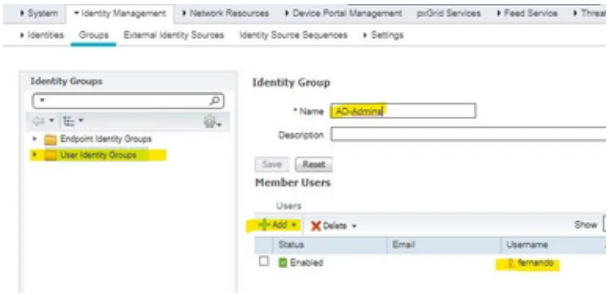
O usuário se autenticou com sucesso e bateu nas políticas padrão de autenticação e autorização.

Vamos agora fechar um pouco nossa política: Na autenticação, permitiremos apenas usuários do AD e, caso eles sejam membros do grupo AD-Admins (que criaremos no ISE), irão se logar e obter **privilégio 15 automaticamente (sem usar senha de enable).**

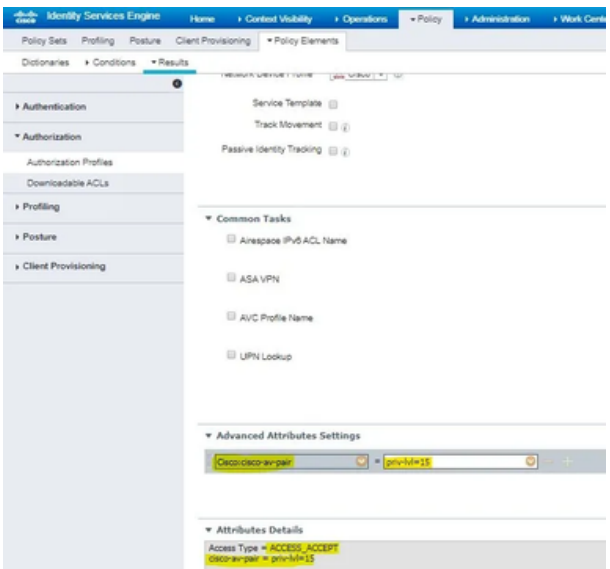
Especificando o AD como única base de usuários para autenticação:



Criando grupo AD-Admins no ISE e adicionando o usuário fernando.



Vamos configurar um Authorization Profile e, usando o atributo **av-pair**, setar o privilégio *(priv-lvl) 15*:

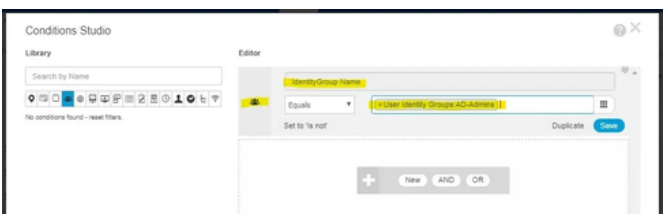


Na política de autorização, criamos uma nova regra e selecionamos esse profile nela:

Ah, reparem na condição *“Identity-AD-Admins”*. Essa condição fui eu que criei e ela simplesmente checa se o usuário faz parte do grupo AD-Admins que criamos acima.

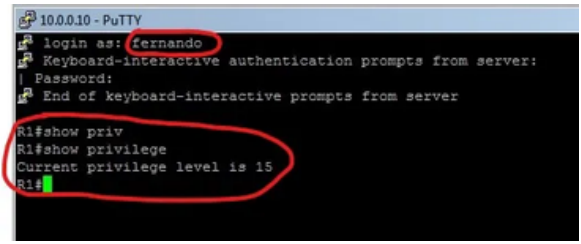
Selecionando a condição *“IdentityGroup Name”*, ao clicar no box abaixo, você seleciona o grupo que você quer e pronto.

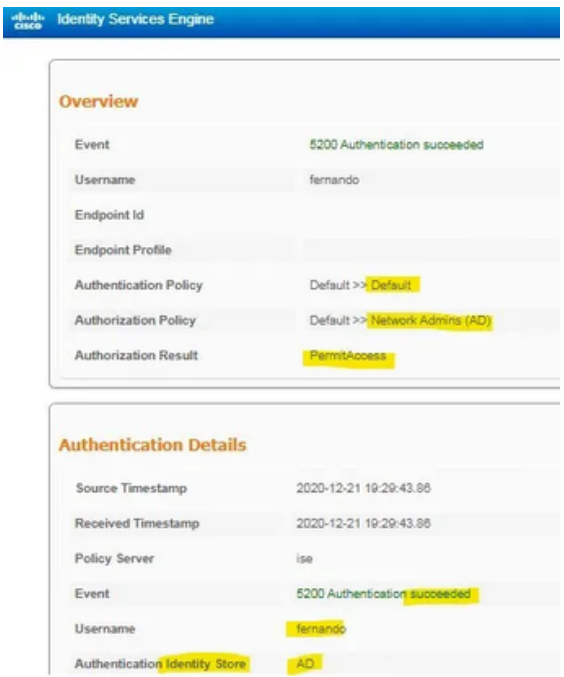
Veja como fica:



E, finalmente, tudo pronto!

Vamos testar? Reparem no privilégio que o usuário recebe ao se autenticar.





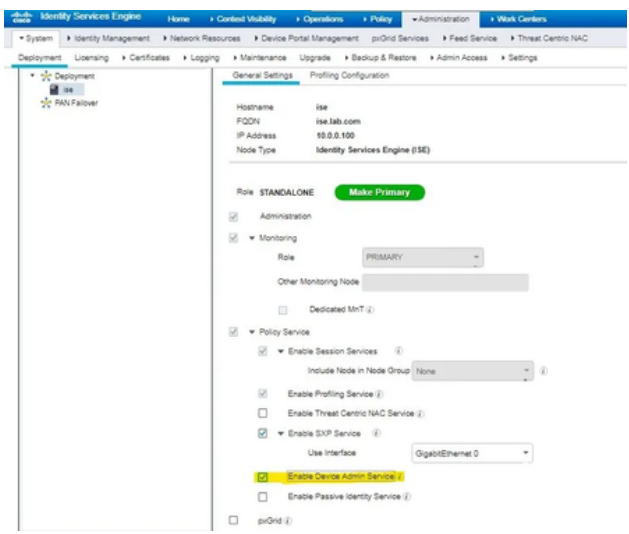
A política de autenticação ainda é a “Default”, mas ela só puxa usuários do AD e não mais de todas as bases configuradas no ISE.

A política de autorização é que a nós criamos: **Network Admins (AD), e entrega privilégio 15 automaticamente para os membros do grupo AD-Admins.**

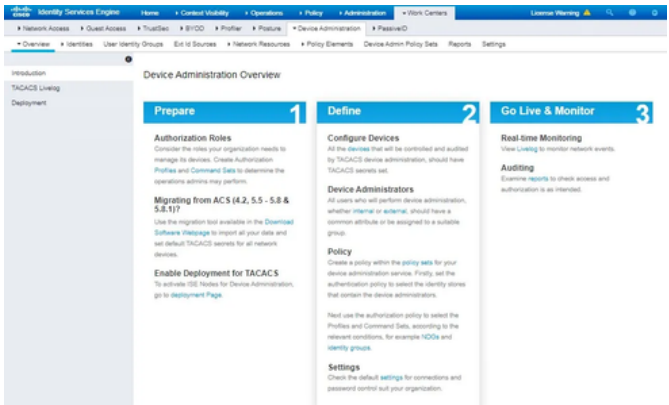
TACACS

Nosso objetivo é permitir que um usuário se logue automaticamente com privilégio 15 mas, de forma granular, permitir apenas alguns comandos específicos.

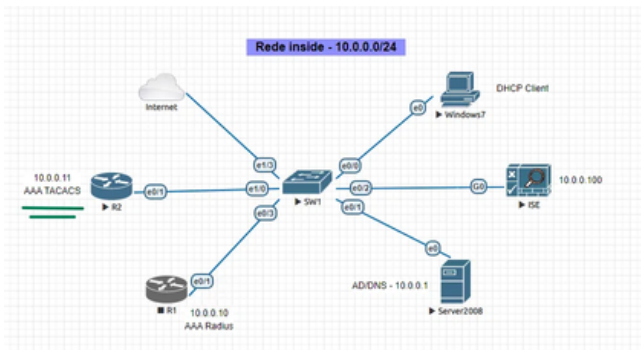
O primeiro passo é ativar o serviço no ISE. Fazemos isso nessa tela:

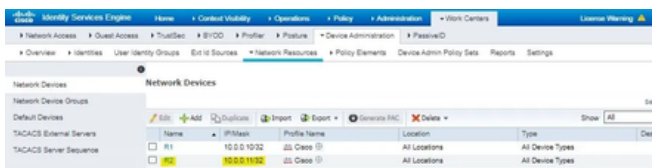


Em seguida, nesse menu, temos uma visão geral dos passos necessários:

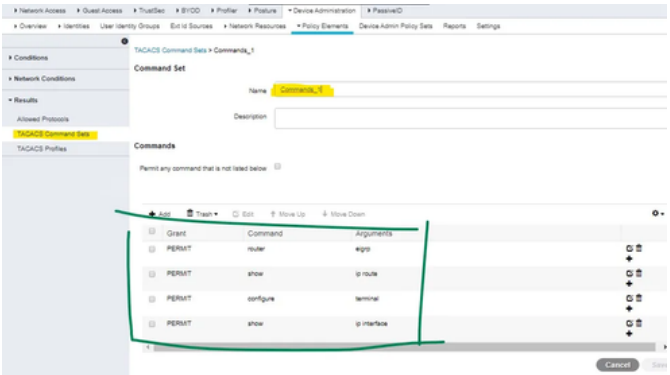


Primeiramente, vamos então adicionar o nosso network device (já fizemos isso nos outros ebooks):

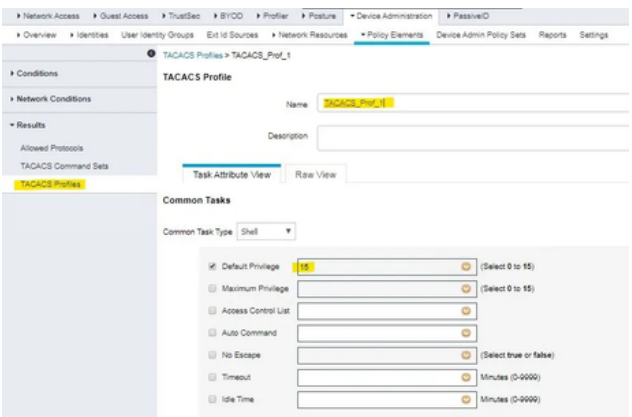




Pronto! Vamos criar agora o *command set* — grupo de comandos que iremos permitir o usuário dar no router. Atente-se à sintaxe, não pode haver erros! Não há checagem por parte do ISE.

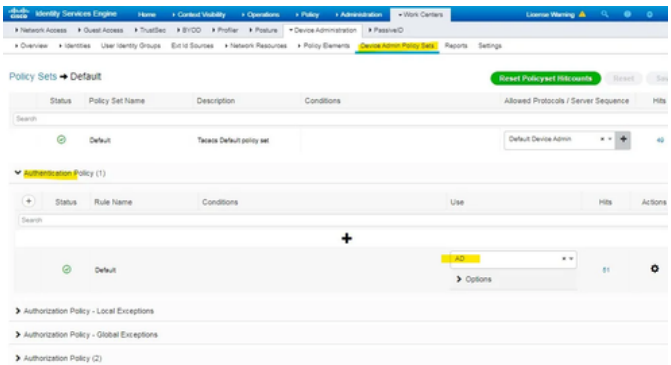


Agora vamos criar o Profile. Repare nos menus. A única informação que vamos colocar é o privilégio 15 automático para o usuário.

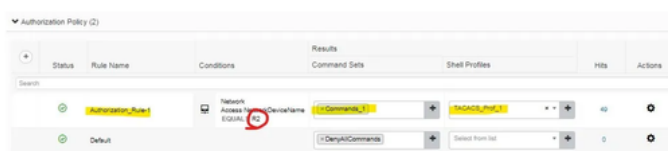


Feito isso, vamos editar a política de autenticação padrão para buscar o usuário apenas no AD que configuramos no artigo passado.

Obs: Repare na estrutura de menu que se trata de outra Policy Set. É uma base de políticas diferente da utilizada pelo Radius. No entanto, elas possuem o mesmo formato.

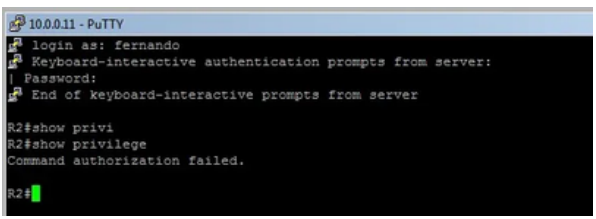


Na política de autorização, nós definimos o *Command Set* que criamos, o *Profile* e, na condição, selecionei apenas o *Network Device* com o nome “R2”. Ou seja, essa condição não se aplica a nenhum outro eqto da rede, apenas a esse router em específico.

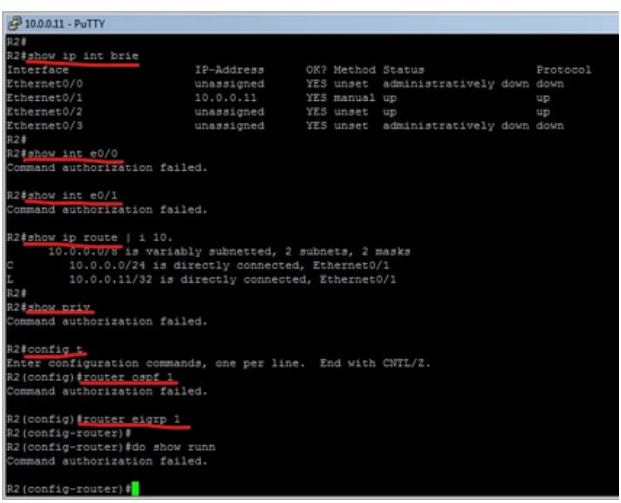


Testando:

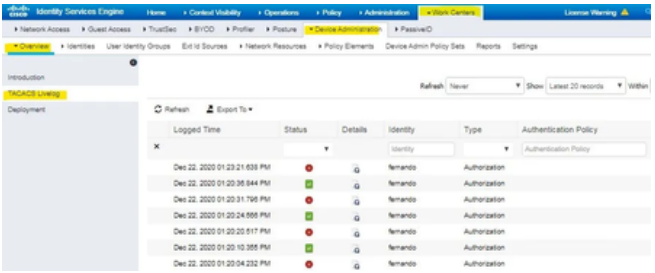
Ao logar, o usuário fernando do AD, recebe direto o prompt privilegiado, mas não é possível entrar com o comando *show privilege*, já que não o permitimos no command set que criamos acima.



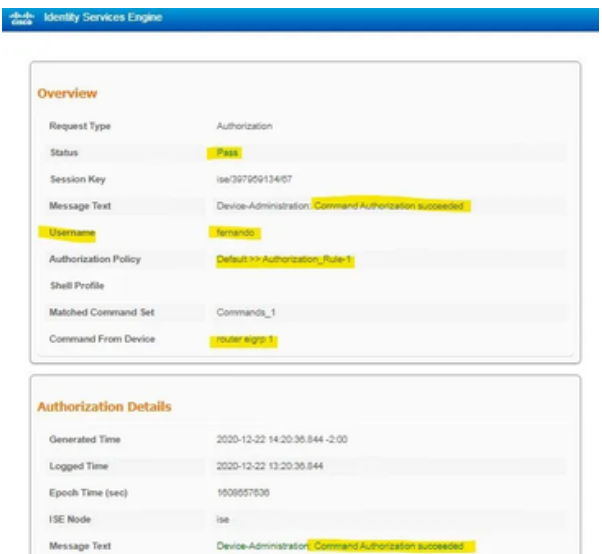
Veja abaixo os comandos que permitimos e os que foram negados. Por ex: não permitimos o *router ospf*, mas permitimos o *router eigrp*.



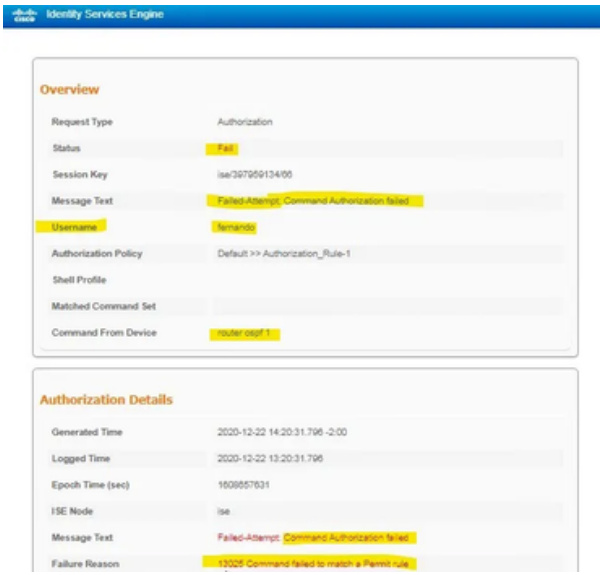
Qto aos logs do TACACS, eles são consultados nesse menu:



Um exemplo de log de comando autorizado:



Um exemplo de log de comando não autorizado:



Por fim, mas igualmente importante a config toda do router(também já detalhada nos ebooks anteriores):

```
aaa new-model
!
!
aaa group server tacacs+ ISE_TACACS
 server name ISE_TACACS
!
aaa authentication login NOAUTH none
aaa authentication login ISE_TACACS group ISE_TACACS
aaa authorization config-commands
aaa authorization exec ISE_TACACS group ISE_TACACS
aaa authorization commands 1 ISE_TACACS group
ISE_TACACS
aaa authorization commands 15 ISE_TACACS group
ISE_TACACS
aaa accounting exec ISE_TACACS start-stop group
ISE_TACACS
aaa accounting commands 15 ISE_TACACS start-stop
group ISE_TACACS
!
interface Ethernet0/1
 ip address 10.0.0.11 255.255.255.0
!
tacacs server ISE_TACACS
 address ipv4 10.0.0.100
 key cisco123
!
line con 0
 logging synchronous
 login authentication NOAUTH
line aux 0
line vty 0 4
 authorization commands 1 ISE_TACACS
 authorization commands 15 ISE_TACACS
 authorization exec ISE_TACACS
 login authentication ISE_TACACS
 transport input ssh
```

Importante destacar 3 comandos nessa config:

```
aaa authorization config-commands
```

“Config-Commands” significa que o network device precisa obter autorização para comandos dados dentro do prompt de configuração (configure terminal)

```
aaa authorization commands 15
ISE_TACACS group ISE_TACACS
```

O “15” significa autorização para comandos de usuários que possuem *privilege level 15*

```
aaa accounting commands 15 ISE_TACACS
start-stop group ISE_TACACS
```

E, finalmente, o *accounting commands 15*, que irá logar cada comando no nível de privilégio 15.

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/