<https://www.freeccnaworkbook.com/blog/ccna-security/cisco-ios-radius-authentication-with-windows-server-2012-nps>

## Cisco IOS autenticação RADIUS com o Windows Server 2012 NPS

Configurando dispositivos Cisco para autenticar usuários de gerenciamento via RADIUS é uma ótima maneira de manter uma base de gerenciamento centralizado de usuários. Tradicionalmente, esta tem sido feito usando o Cisco Access Control Server (ACS), que, claro, é bastante caro e é tipicamente fora da faixa de preço para a maioria das pequenas e médias empresas.

Se você é como a maioria das empresas que você já pode ter uma infra-estrutura Active Directory implantado e, assim, você já tem o software e as licenças necessárias e exigidas para configurar um servidor RADIUS básico usando Network Policy Server (NPS), que pode ser usado para autenticar os administradores de rede em seu Cisco equipamentos IOS para fins de gestão. O principal benefício que você começa de autenticação RADIUS é um console de gerenciamento centralizado para autenticação do usuário ea capacidade de controlar quais usuários têm acesso ao Cisco CLI. Então, olhando por este caminho; se a sua empresa contrata ou dispara um empregado do que o que quer que as alterações são aplicadas no Active Directory terá efeito imediatamente. Como a desativação de uma conta de usuário no AD resultaria em tentativas de autenticação falhadas para esse nome de usuário ao tentar fazer logon em um dispositivo Cisco. Além disso, se você tem um novo funcionário, você pode facilmente dar o seu acesso nome de usuário para dispositivos de rede Cisco apenas adicionando-os em um grupo de segurança no Active Directory.

Este blog vai discutir e demonstrar a configuração do Network Policy Server, que está incluído no Windows Server 2008 e maior no entanto vai blog concentrar no Windows Server 2008 R2.

## Configuração do Active Directory

Primeiro, há uma pequena tarefa poucos você deve concluir no Active Directory. Você deve criar dois grupos de distribuição de segurança chamado engenheiros de rede e suporte de rede Técnicos

Engenheiros de rede terá de nível 15 privilégios e, portanto, tem permissões de leitura / escrita completa para a interface de linha de comando Cisco depois de autenticar com sucesso para roteadores e switches Cisco.

Técnicos de Suporte de Rede no entanto, apenas terá de Leitura privilégios.

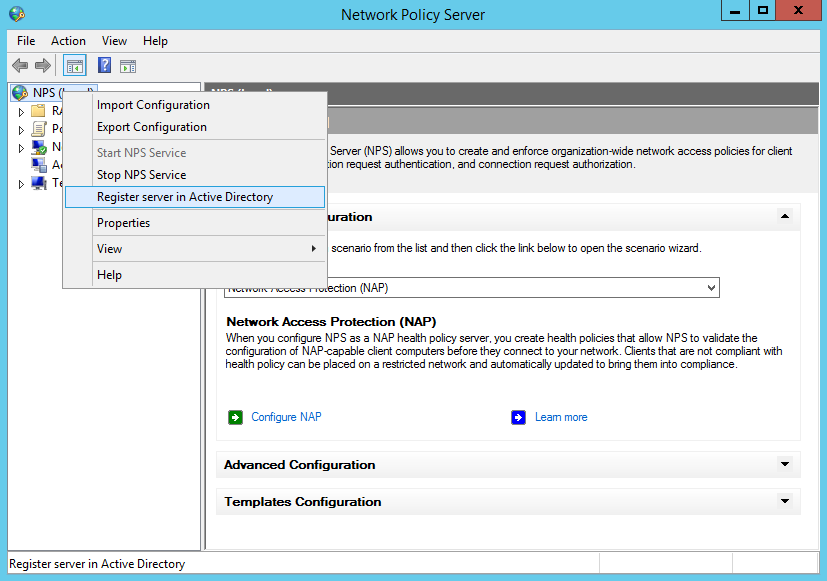
Em seguida, você terá de atribuir usuários a esses grupos. Para os fins deste blog eu criei dois usuários, John Doe e John Smith.

John Doe (Nome de usuário: jdoe) é um engenheiro de rede e John Smith (Nome de usuário: jsmith) é um técnico de suporte de rede. Esses usuários serão utilizados para verificar a configuração e status operacional do NPS.

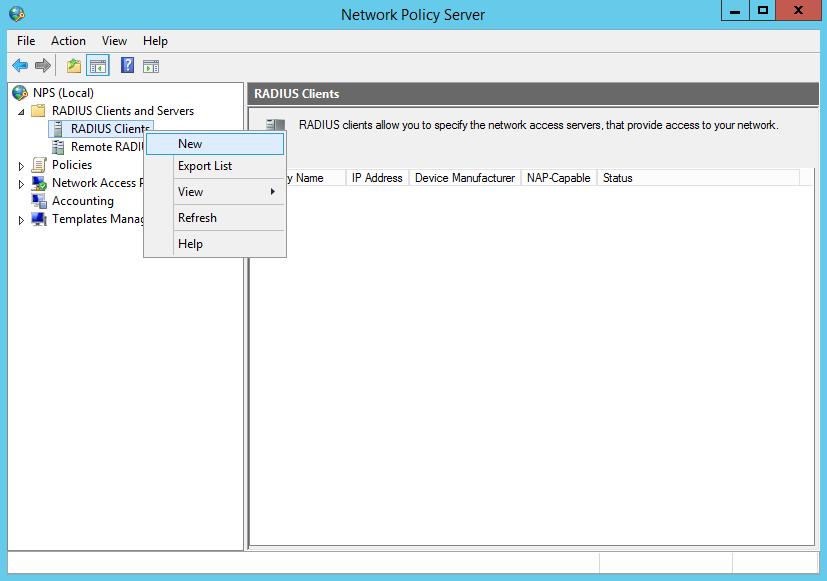
Depois de ter concluído a configuração básica do Active Directory, você pode passar para a configuração do NPS. Por favor note que os grupos de segurança pode ser chamado o que quiser.

## Configuração de rede do Windows Policy Server

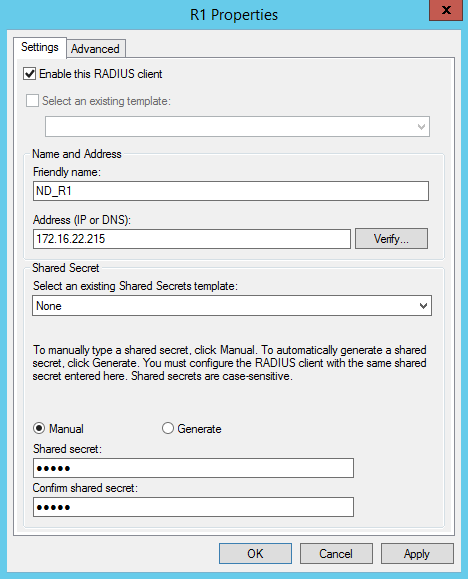
Antes de configurar o NPS ele deve primeiro ser instalados e autorizados no Active Directory. Para instalar o NPS adicionar a função de "Política e Acesso Serviços de Rede" para seu servidor.



Depois de ter autorizado NPS no Active Directory que você está pronto para adicionar o primeiro cliente RADIUS. Para adicionar o cliente tem de expan a linha de clientes RADIUS e servidores e clique direito sobre Clientes RADIUS e clique em "Novo".

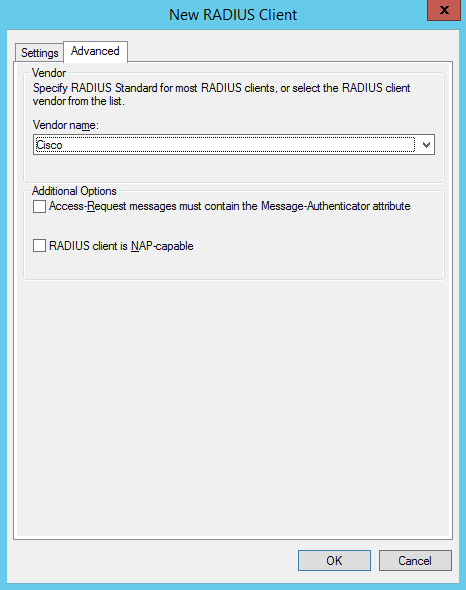


Você será solicitado a digitar o nome amigável e endereço, endereço de IP e segredo compartilhado.Inserir essas informações, conforme necessário. Para este blog estamos usando R1 que tinha o endereço IP 172.16.22.215 e o segredo da CISCO, como mostrado abaixo;

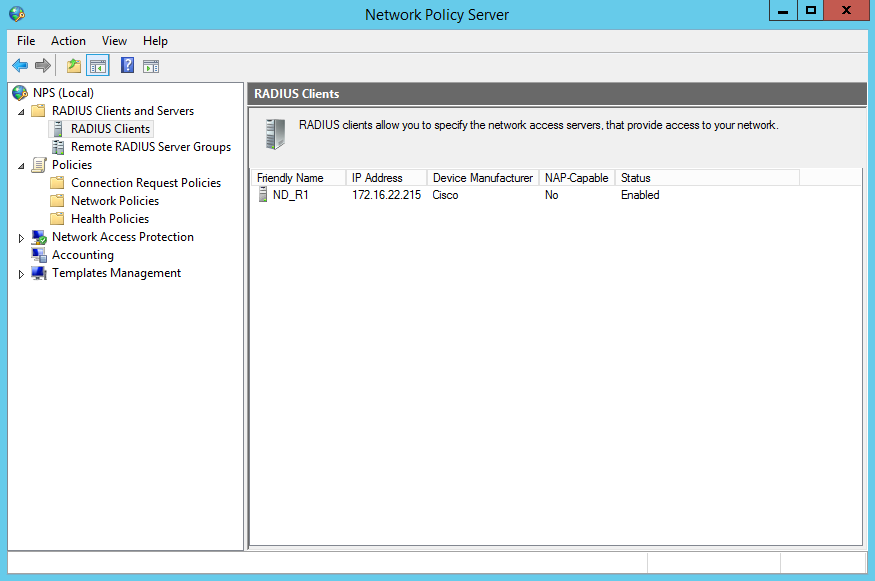


Note-se que ND\_ é utilizado como um prefixo para o nome amigável dispositivo, este vai ser usado mais tarde na configuração da Política de NPS que possa identificar os dispositivos de rede.

Em seguida, clique na guia Avançado em todo o tipo e selecione "Cisco", como o nome do fornecedor da lista suspensa e clique em OK;

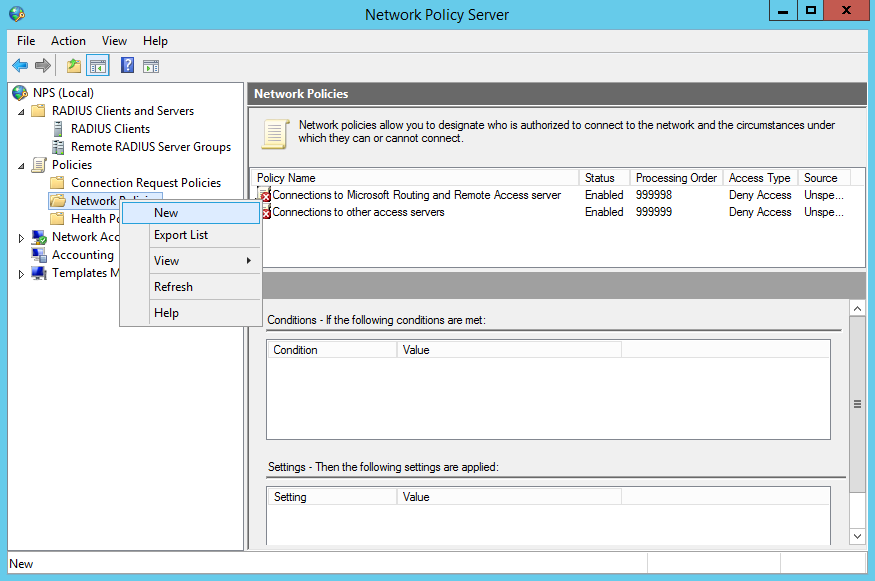


Se você adicionou o cliente corretamente, você deve ver o nome amigável do cliente, endereço IP e outras informações listadas na seção Clientes RADIUS;

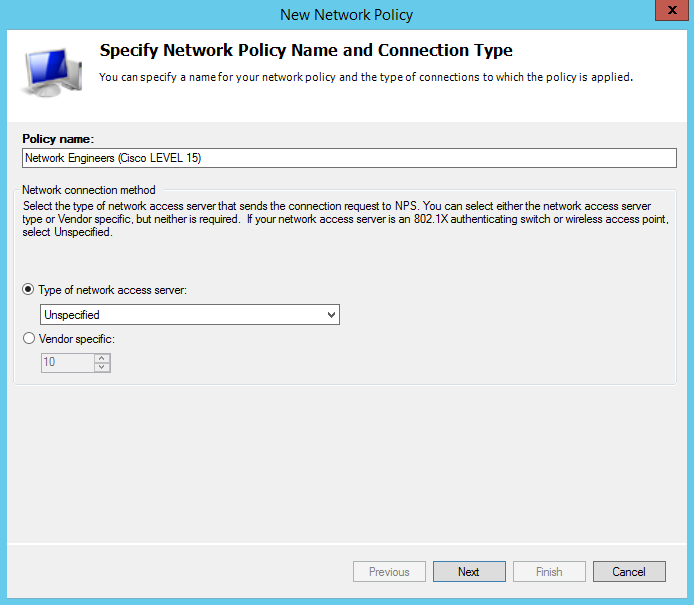


Agora você está pronto para configurar a política de rede que irá autenticar os usuários nos grupos específicos do Active Directory e conceder-lhes acesso.

para criar uma nova política que você precisa para expandir o item Políticas na lista à esquerda e clique direito sobre "Políticas de Rede" e clique em Novo.



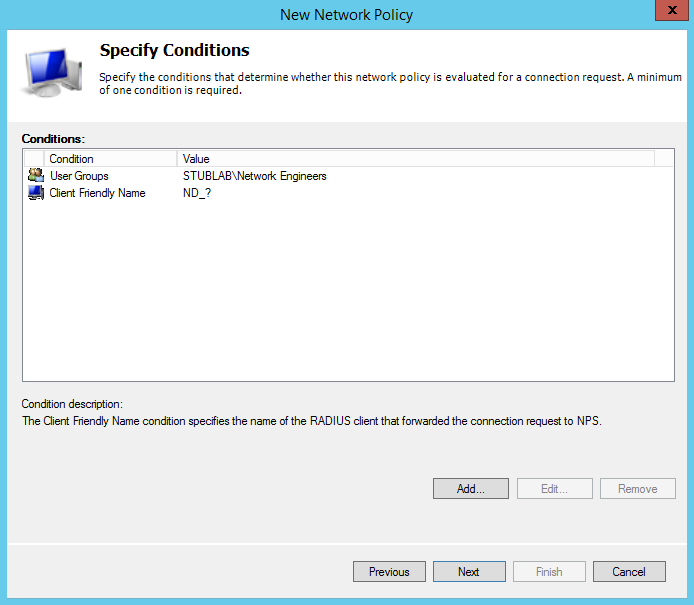
Você deve digitar um nome para a política, neste caso vamos usar "Network Engineers (Cisco NÍVEL 15)"



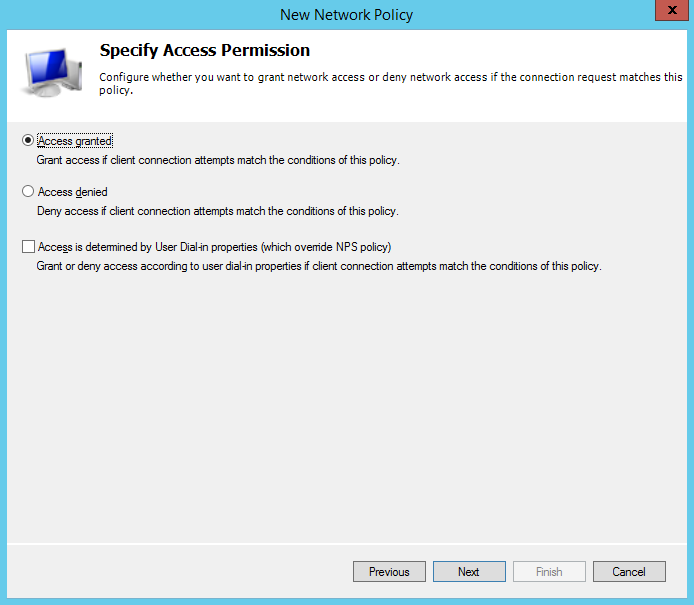
Depois de ter fornecido um nome de política que você deve de configurar as condições que são necessárias para corresponder, a fim de autenticar com êxito. Você vai precisar para criar duas condições;

Configurar um grupo de usuários para coincidir com o grupo de segurança engenheiros de rede e o amigável Nome do cliente para corresponder "ND\_?", Que denota a autenticação do dispositivo tem um nome amigável começando com ND\_

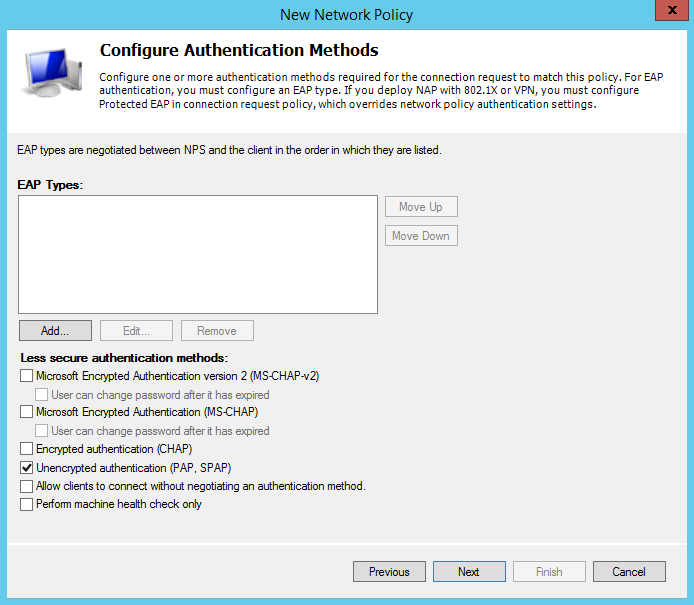
Depois de adicionar com êxito estas condições que você deve ver o seguinte;



Clique ao lado e você será solicitado a especificar a permissão de acesso, deixe este como padrão "Acesso concedido" e clique em Avançar.

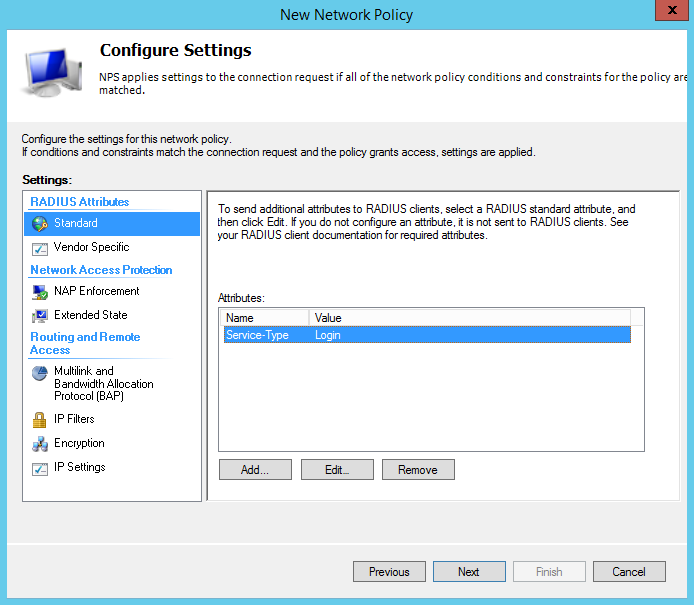


Cisco suporta apenas o "autenticação não criptografada (PAP, SPAP) métodos. Desmarque tudo e marque a opção "autenticação não criptografada (PAP, SPAP) como mostrado abaixo e clique em Avançar;



Depois de configurar os métodos de autenticação que você será solicitado a configurar as Constraits, você pode pular esta seção e basta clicar seguinte.

Quando solicitado a configurar as definições, remova o Framed-Protocol e editar o Service-Type e defina-o "Login" que está sob "Outros" como mostrado abaixo;

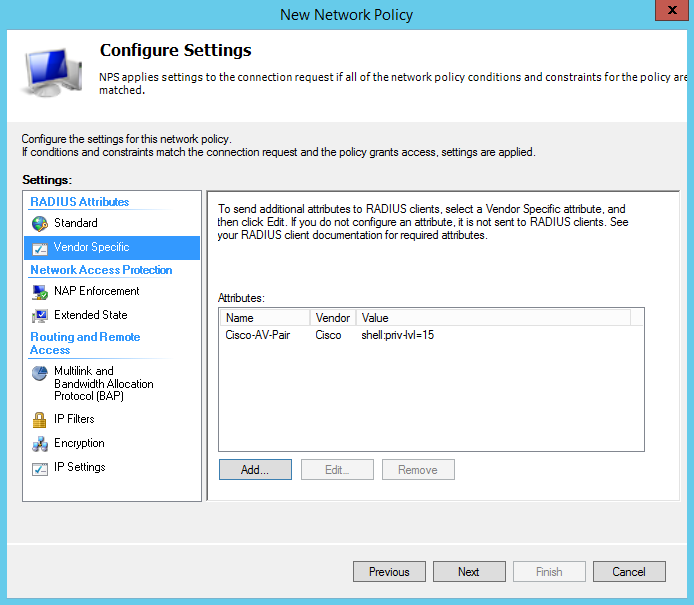


Em seguida, você vai precisar adicionar um Fornecedor atributo específico clicando em "fornecedor específico" sob as configurações do lado esquerdo e clicando no botão Add ...

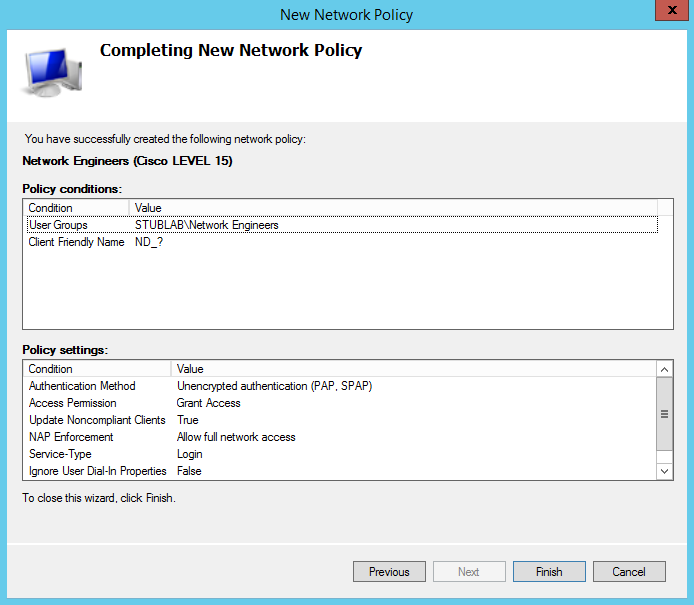
Role a lista e selecione "Cisco-AV-Pair" e clique em adicionar. Você será solicitado para adicionar o atributo da Informação, aqui você vai clique em Adicionar ... e definir o valor do atributo como shell: priv-lvl = 15

Isto especifica que o nível de privilégio é devolvido ao usuário de autenticação / dispositivo após a autenticação bem-sucedida. Para os engenheiros de rede este seria shell: priv-lvl = 15 e os Técnicos de Suporte de Rede usaria shell: priv-lvl = 1

Quando adicionado com sucesso, você deve ver o seguinte;



Depois de clicar em seguinte, você será apresentado um resumo da nova política de rede que você acabou de criar, como mostrado abaixo;



Clique em Concluir e você está pronto co configurar os roteadores e switches da Cisco para autenticar o NPS Radius Server. Por favor, note que você vai precisar para criar outra política para os técnicos de suporte de rede e quaisquer outros níveis de privilégios que você deseja usar.

**Configuração Cisco**

**Switch:**

Now it’s time to work on the Cisco device.

First I’d suggest setting up some basic security settings as follows:

**Switch>enable  
Switch#configure terminal  
Switch(config)#aaa new-model  
Switch(config)#username xxxx secret xxxx  
Switch(config)#enable secret xxxx  
Switch(config)#crypto key generate rsa  
Switch(config)#ip ssh time-out 60  
Switch(config)#ip ssh version 2  
Switch(config)#line vty 0 4  
Switch(config-line)#transport input ssh  
Switch(config-line)#exit  
Switch(config)#line vty 5 15  
Switch(config-line)#transport input ssh  
Switch(config-line)#exit**

The above turns on the new aaa model, creates a user with a password, sets an enable password and turns on ssh version 2 (you do have PuTTY don’t you?).

Now it’s time to configure the device to communicate with the RADIUS server:

**Switch(config)#ip domain-name foo.com  
Switch(config)#radius-server host x.x.x.x  
Switch(config)#radius-server key xxxxxxxxxxxxxxxxx (this is where you paste in the shared secret from above)  
Switch(config)#aaa group server radius NPSSERVER (You can put whatever you want for NPSSERVER)  
Switch(config-sg-radius)#server x.x.x.x  
Switch(config-sg-radius)#exit  
Switch(config)#aaa authentication login default group NPSSERVER local  
Switch(config)#aaa authorization exec default group NPSSERVER local  
Switch(config)#exit  
Switch#**

Before you copy the running config to the startup open PuTTY and type in the IP address of the device. You will be presented with a login as: prompt followed by a password prompt. Use your regular AD login credentials (hopefully you’re in the AD group you selected above when creating the network policy) and if all goes well you’ll be presented with a privileged command prompt. The privileged command prompt is the result of two things. First the policy specified a Cisco-AV-Pair of shell:priv-lvl=15.  Second the aaa authorization exec line tells the Cisco device to get your authorization level from the NPSSERVER group.

Now there are other ways to configure the Cisco device and get the same results. Instead of specifying the radius-server host outside the group you could add it within the group like this.

**Switch(config)#aaa group server radius NPSSERVER (You can put whatever you want for NPSSERVER)  
Switch(config-sg-radius)#server x.x.x.x key xxxxxxxxxxxxxx  
Switch(config-sg-radius)#exit**

**ROTEADOR**

Configuração AAA Cisco IOS

A primeira coisa que precisamos fazer antes de configurar AAA é a configuração de uma conta de usuário local para que quando o servidor RADIUS falhou, você tem a capacidade de ainda fazer login no dispositivo. Isso é feito usando o comando nome de usuário, como demonstrado abaixo;

R1 con0 is now available

Press RETURN to get started.

R1>enable

R1#config terminal

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)#username NORAD priv 15 secret R@du3F@1led

R1(config)#

Agora podemos permitir AAA novo modelo e configurar o grupo de servidor RADIUS e lista de autenticação padrão, como demonstrado abaixo;

R1(config)#username NORAD priv 15 secret R@du3F@1led

R1(config)#aaa group server radius NPS\_RADIUS\_SERVERS

R1(config-sg-radius)#server-private 172.16.22.228 auth-port 1812 acct-port 1813 key CISCO

R1(config)#aaa authentication login default group NPS\_RADIUS\_SERVERS local

R1(config)#aaa authorization exec default group NPS\_RADIUS\_SERVERS local if-authenticated

R1(config)#aaa authorization console

INFO: os usuários só poderão autenticar os servidores RADIUS se o servidor RADIUS está vivo na definição da lista de autenticação aaa padrão usando NPS\_RADIUS\_SERVERS grupo seguido de local. Se você está tentando efetuar login no dispositivo usando uma conta local e os servidores RADIUS são facilmente acessível do que irá rejeitar a autenticação, a menos que a conta local usado para efetuar login também existem no Active Directory e são membro (s) da Ordem dos Engenheiros de rede ou de rede Técnicos de suporte grupo de segurança.

E isso é tudo para o básico de configuração Cisco IOS AAA. No entanto, pode entrar em algumas configurações mais avançadas usando lista AAA e aplicar uma lista de autenticação raio para as linhas VTY e autenticação local somente para a linha de console.