NPS - Network Policy Server

- Créditos
- Introdução
  - Breve explicação do processo
- Requisitos
- Instalação do serviço de NPS
- Autenticação / Autorização no NPS - Eduroam
  - O Cenário
- Configuração
  - RADIUS Clients
  - Remote Radius Server Groups
  - Connection Request Policies
    - Autenticação de Roamers
  - Network Policies
    - Autenticação de alunos internos na rede eduroam
      - Condições
      - Restrições
      - Perfil
      - Separador Overview
    - Autenticação de utilizadores internos em Roaming
    - Descarte com resposta dos pedidos mal formatados
- Geração de Certificado de validação do servidor
  - Criação do pedido de certificado
  - Aceitação, Instalação e Validação do Certificado
- Anexos
  - Importação da Base de Dados do IAS para o NPS
    - Considerações
    - Transferência da BD do IAS para o NPS
  - Transferência de Certificado de Validação do Servidor

Créditos

Este documento, que decreve em detalhe o processo de instalação e configuração do servidor de RADIUS Network Policy Server (NPS) para a rede eduroam, foi escrito e disponibilizado pela Universidade de Aveiro em 10 de Janeiro de 2010.

Introdução

O Network Policy Server (NPS) é um servidor RADIUS comercial que implementa a norma RADIUS IETF. Este serviço é incluído no Windows 2008 Server substitui o Internet Authentication Service (IAS).

Neste documento são descritos os seguintes procedimentos:

- Instalação do serviço de NPS num novo servidor
- Explicação da configuração pormenorizada e personalizada das regras de Autenticação e Autorização de utilizadores na rede eduroam.
- Importação da base de dados do IAS para o NPS;

Breve explicação do processo

Para que um Utilizador consiga ligar-se à rede wireless e o processo possa ser monitorizado é necessário que existam e estejam corretamente configurados os seguintes itens ao nível do NPS:

- Registo do NPS na AD – após corretamente configurado o nome e domínio do servidor RADIUS, faz-se o registo do servidor na AD pelo interface do NPS, para que este seja visto como um servidor de autenticação legítimo e possa consultar livremente os grupos e users.
- Os **NAS (Access Points no caso**) são registados como **RADIUS clientes** no NPS configurando um nome (**Client Friendly Name**), um IP e uma **Shared Secret** de estabelecimento da associação de segurança entre NPS e NAS.
- O pedido de autenticação recebido pelo NAS passa primeiro pelas **Connection Request Policy** que são regras que avaliam se o pedido vai ser correlacionado com as regras de autenticação locais ou encaminhado a qualquer outro servidor de autenticação remoto.
- O NPS trata um pedido comparando os atributos recebidos no pedido de autenticação com as **Network Policies**, que são as regras de autenticação ordenadas onde vigoram as diversas condições que qualificam um utilizador como apto ou não ao acesso à rede wireless, e o perfil de saída aplicado por essa regra (ex: marcação da VLAN).
- Cada evento de autenticação gera logs de sistema que podem consultar-se no **EventViewer**. O **Logging** é também configurado no NPS e gera um ficheiro diário de logs (em c:\windows\system32\logfiles\inAAMMDD.log) com todas as mensagens RADIUS trocadas entre o servidor e os clientes.

Requisitos

A instalação do NPS pode ser feita apenas em servidores Microsoft Windows 2008. Os requisitos mínimos necessários para instalar o sistema operativo são:

- Processador: 1.4 GHz 64-bit;
- RAM: mínimo 512 MB;
- HD: mínimo 32 GB.

Nota: O NPS do Windows 2008 R2 Server Standard tem um limite máximo de 50 clientes RADIUS (autenticadores, neste caso APs).

Instalação do serviço de NPS

Enumeram-se de seguida os passos tomados na instalação e configuração do sistema RADIUS:

- Instalar Windows Server 2008 R2 Enterprise;
- Instalar os Service Packs, HotFixs e Updates necessários;
- Adicionar o servidor ao domínio
- Instalar o NPS
    - Start -> Administrative Tools -> Server Manager
    - RightClick em Roles -> Add Roles
    - Escolher o serviço “Network Policy and Access Services”
    - Findo este ponto o servidor NPS está instalado.

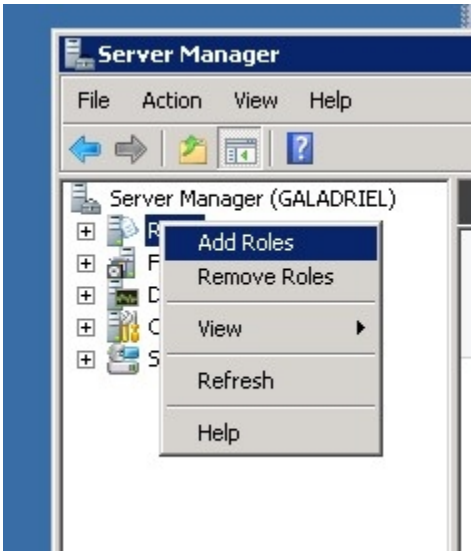


Figura 1: Ativação do serviço de NPS

Pode agora lançar-se o serviço de NPS:

- Start->Administrative Tools-> Network Policy

É aberta a mmc com o snap-in do NPS. Rightclick sobre NPS(local) e selecionar a opção Stop NPS Service do drop-down menu para parar o serviço para configuração.

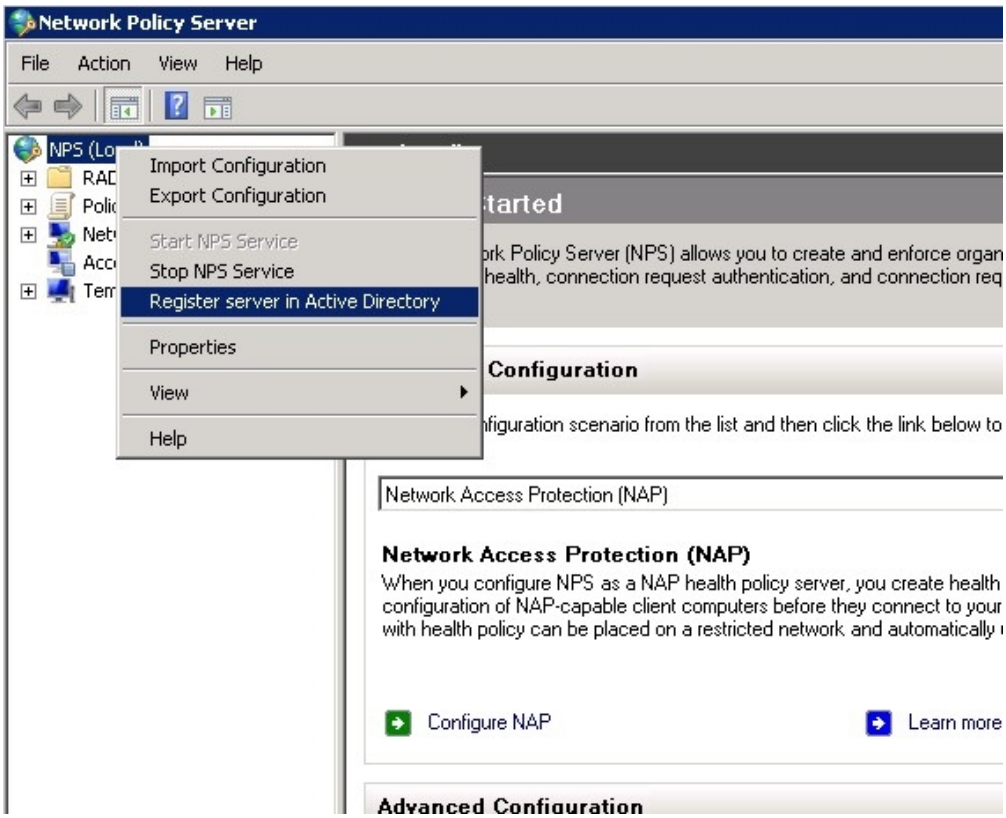


Figura 2: Snap-in do NPS

Autenticação / Autorização no NPS - Eduroam

O Cenário

A configuração do NPS foi realizada tendo em vista as características de mobilidade a implementar na rede eduroam, contemplando também algumas particularidades da Universidade de Aveiro.

Como requisitos principais para o cenário foram definidos os seguintes:

- Suporte de realms (user@instituição.pt)
  - Do tipo @ua.pt para os utilizadores da Universidade de Aveiro;
  - Do tipo @instituição.país para utilizadores externos em roaming;
- Suporte de proxy RADIUS
  - Para redireccionamento dos pedidos de autenticação e auditoria de utilizadores externos à UA
- Atribuição de VLANs por perfil de utilizador
  - Alunos
  - Staff
  - Roamers
- Suporte de um SSID “eduroam” com 802.1x (WPA)
  - Para autenticação através de PEAP / MS-CHAP-V2
  - Com atribuição de perfis de utilização

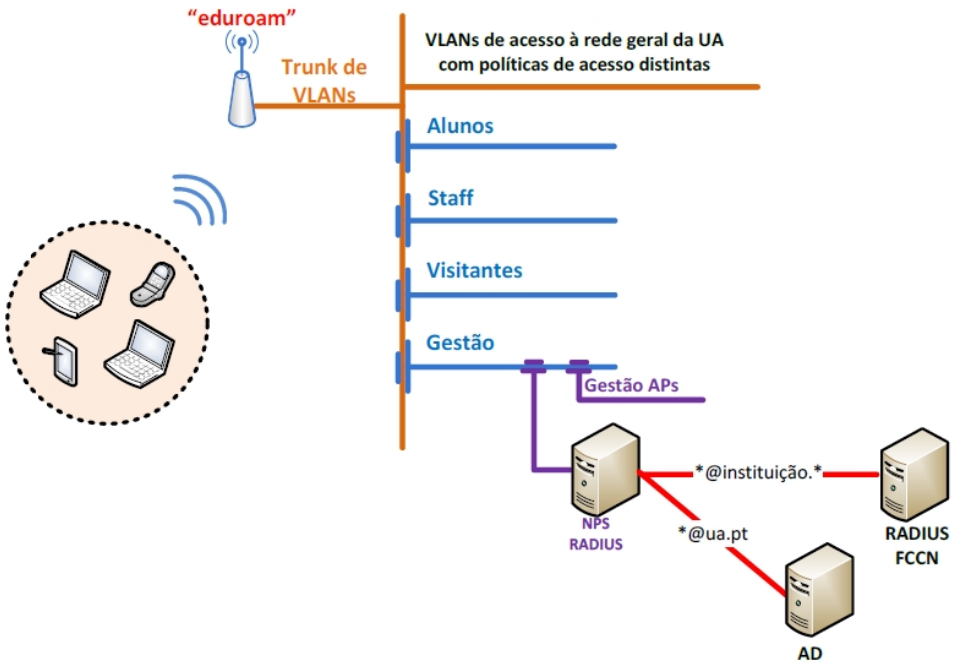


Figura 3: Esquema geral do cenário

A rede é difundida sob o SSID "eduroam", onde qualquer utilizador pertencente a qualquer universidade se pode autenticar. Segundo o vínculo do utilizador para com a Universidade de Aveiro, o RADIUS autentica o utilizador e coloca-o numa rede (VLAN) específica, seja ela a rede de alunos, staff ou visitantes externos.

Para além de outras funções, a rede de gestão de APs transporta os pedidos de autenticação entre os APs e o RADIUS, sem necessidade de routing (mesma LAN).

Configuração

RADIUS Clients

Na interface de gestão do NPS devem configurar-se diversos parâmetros de forma a capacitar a rede com as ferramentas disponibilizadas por este serviço.

- **APs**: devem ser configurados como Radius Clients para que possam comunicar com o NPS. Tal pode ser feito individualmente para cada um dos equipamentos ou usar máscaras que agrupam porções de endereços de rede correspondentes aos IPs de gestão dos APs. Por exemplo, para todos os IPs da rede 192.168.2.0, "Client IP" = "192.168.2.0/24") os APs podem agrupar-se por departamento, edifício, zona, etc. É configurada também a Shared Secret que foi previamente definida nos APs, permitindo a autenticação destes como RADIUS Clients no NPS.
- **FCCN RADIUS**: Este cliente é definido para permitir o encaminhamento e receção de pedidos de autenticação de utilizadores em Roaming.

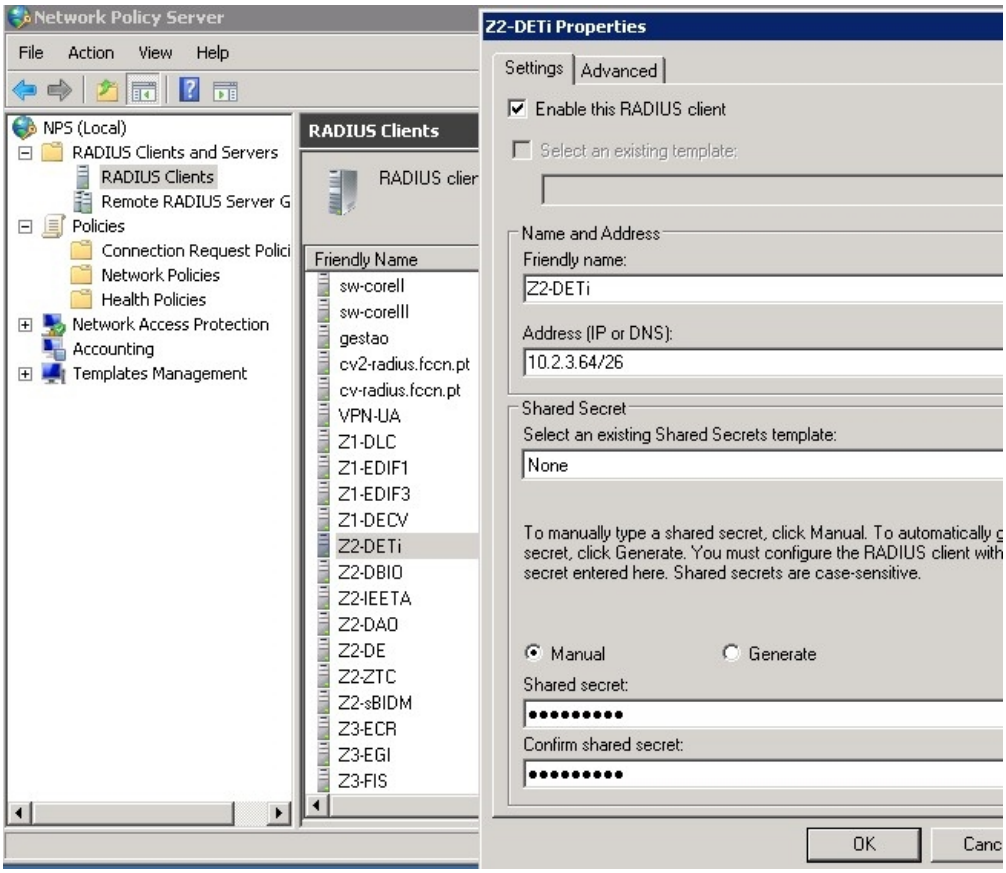


Figura 4: Adicionar um RADIUS Client

- **Procedimento**: Selecionar “New RADIUS Client” com RightClick do rato, escolher o “Friendly Name” estratégico tomando em atenção a política de nomes elaborada de acordo com as necessidades/especificidades da Instituição, facilitando a elaboração de expressões regulares empregues nas políticas de acesso e debugging. Configurar IP ou segmento de rede e introduzir a Shared Key.

Nota: Segundo as recomendações da **Eduroam Operations Team**, no documento “**Admin Advisory-004 May 2011**”, os **RADIUS clients** devem especificar o **vendor name** como **RADIUS Standard**, nas configurações avançadas dos clientes.

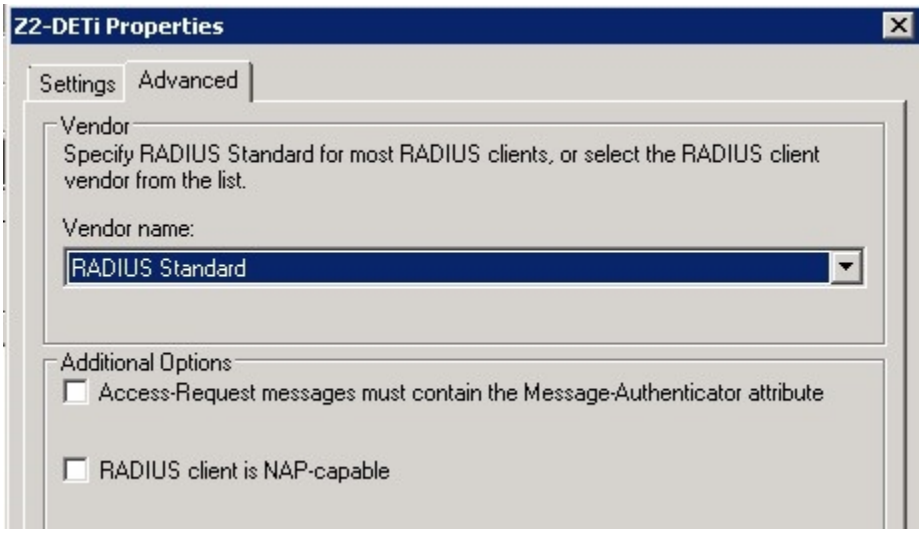


Figura 5: Configuração recomendada para "vendor name"

Remote Radius Server Groups

Nesta opção são definidos os servidores PROXY de RADIUS, para onde podem ser encaminhados os pedidos de autenticação. No cenário é definido um grupo FCCN, com os servidores **cv-radius** da FCCN com os portos de autenticação TCP/UDP 1812 e accounting TCP/UDP 1813.

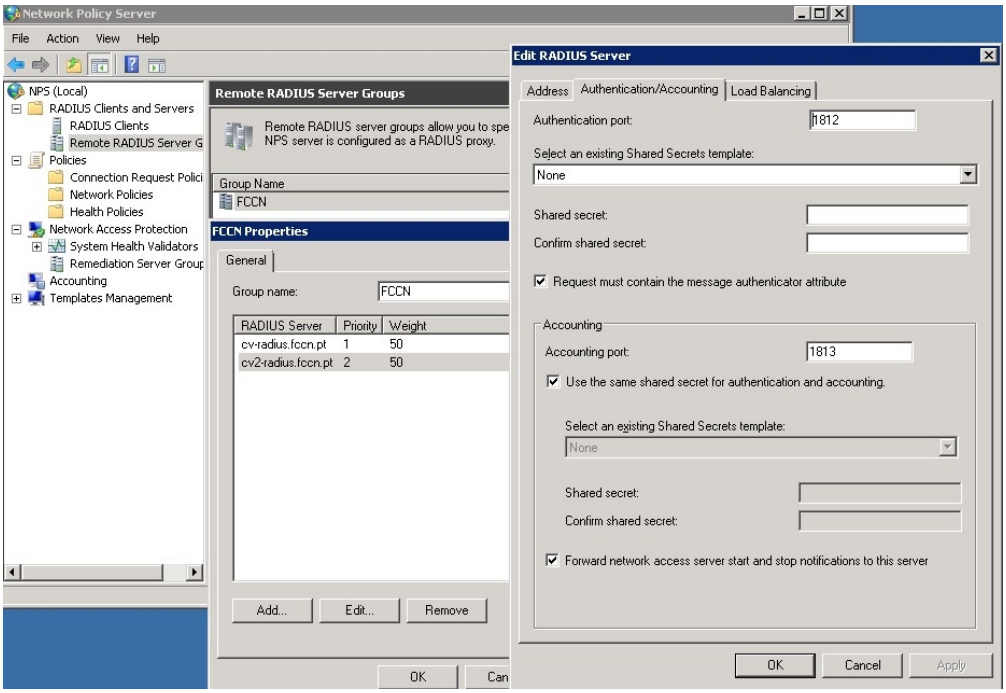


Figura 6: Configuração de servidores RADIUS remotos

Nota: Uma vez que pedidos de autenticação de utilizadores internos em roaming nas outras instituições são encaminhados para o servidor RADIUS local pelo servidor remoto da FCCN, então esse servidor remoto, além de proxy RADIUS também deve ser definido como cliente, com atribuição de **Friendly Name** , tal como é feito para os APs.

Connection Request Policies

Dependendo dos atributos constantes nos pedidos de autenticação RADIUS, o servidor determina se os pedidos sofrem a autenticação num servidor remoto, ou se é ele próprio o responsável pelo processo de autenticação.

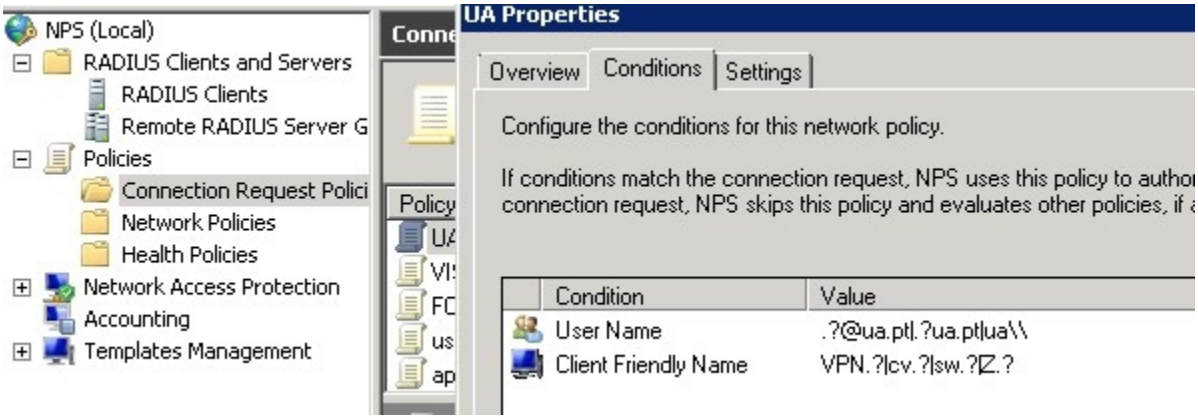


Figura 7: Connection request policy para autenticação local

A imagem anterior demonstra as condições para realização da autenticação local. O atributo de **User Name** deve conter o domínio **ua.pt** (ou ua\username). O **Client Friendly Name** é validado se for feita a autenticação via APs ou via **cv** (proxys da FCCN).

A imagem seguinte demonstra a configuração dessa **connection request policy** para autenticação local.

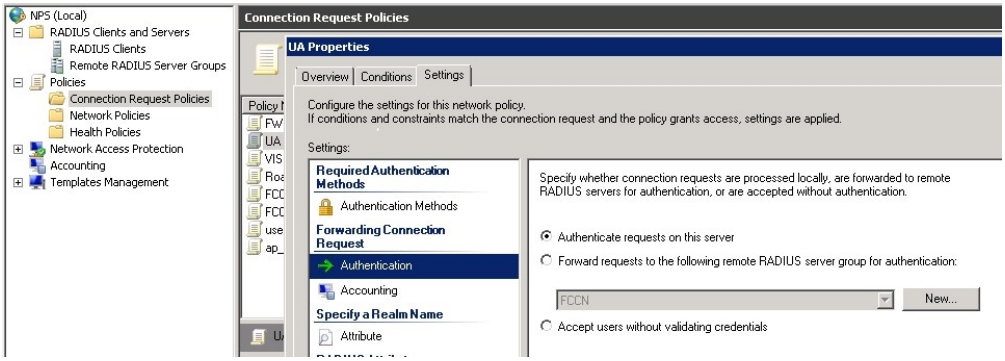


Figura 8: Especificação do alvo de autenticação

Autenticação de Roamers

As configurações para autenticação de alunos de instituições externas a usar a eduroam na UA são feitas ao nível das **Conection Request Policies**.

Para autenticação de roamers de outras instituições na rede eduroam da UA é necessário:

- Verificação do username;
- Encaminhamento de pedidos de autenticação válidos para o proxy remoto;
- Encaminhamento do accounting para a fccn;
- Marcação de VLAN local após autenticação remota bem sucedida.

A imagem seguinte mostra a regexp que seleciona os pedidos que devem ser direcionados aos proxys da FCCN.

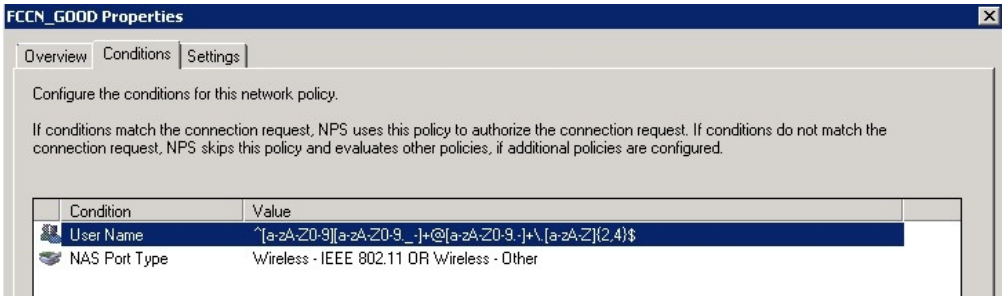


Figura 9: Connection request policy para autenticação remota

^[a-zA-Z0-9][a-zA-Z0-9._-]+@[a-zA-Z0-9.-]+\.[a-zA-Z]{2,4}$

Para ser enviado para a FCCN o login tem de cumprir as seguintes regras:

- Primeiro carater seja uma letra ou numero
- Tem pelo menos dois carateres antes do @ que poderão ser letras, números e “._-“
- Tem um @
- Tem pelo menos um domain antes do TLD
- O TLD tem entre 2 a 4 carateres só com letras.

Se o pedido de autenticação cumpre com as condições anteriores, é então encaminhado para um proxy remoto do **Remote RADIUS Server Group** configurado anteriormente:

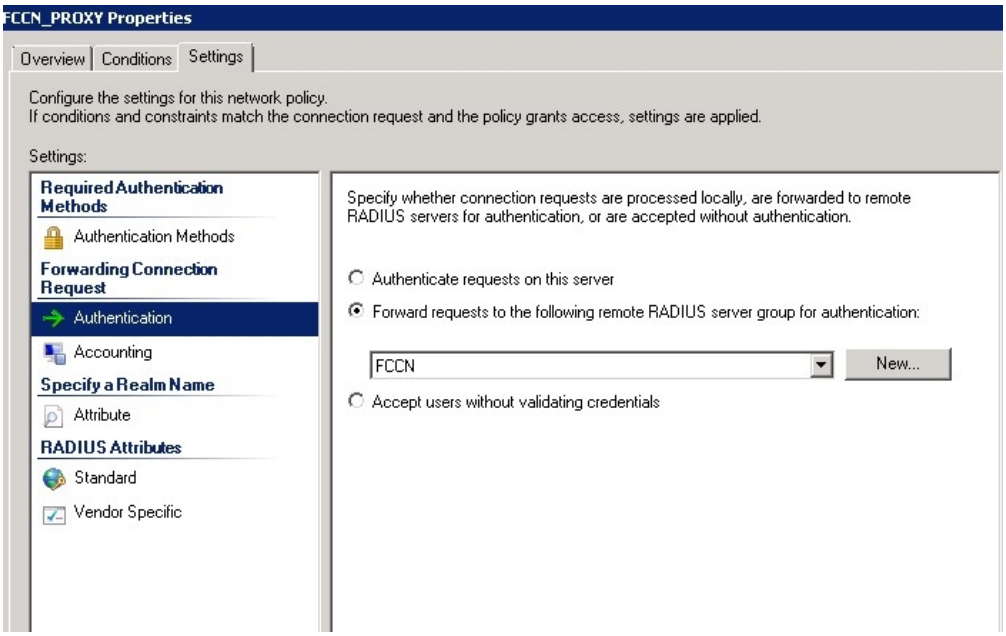


Figura 10: Encaminhamento do pedido de autenticação

Também deve ser enviada informação de accounting para o mesmo servidor remoto, selecionando a opção mostrada abaixo e escolhendo o mesmo grupo de servidores remotos que na autenticação.

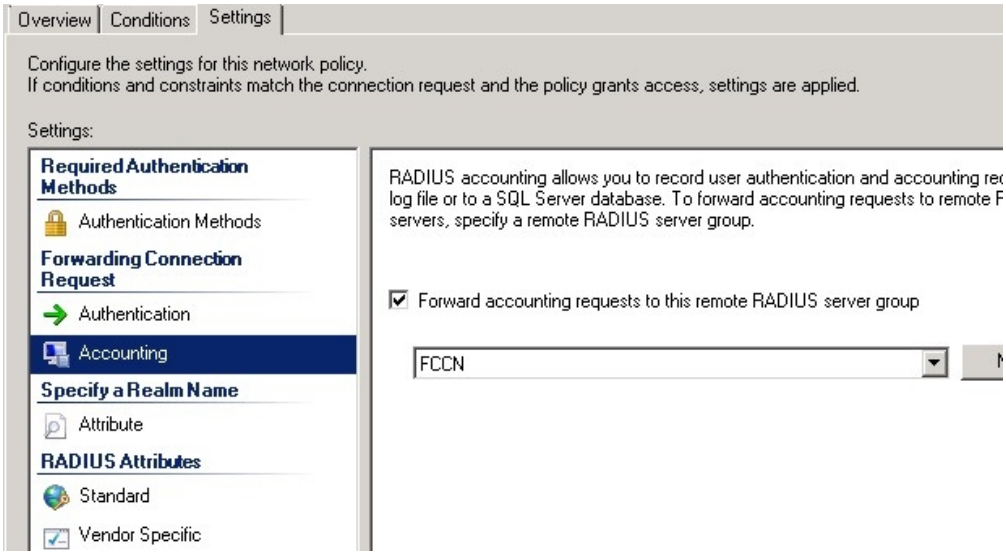


Figura 11: Encaminhamento da informação de accounting

Quando a autenticação é finalizada no servidor remoto, e caso seja bem-sucedida, o utilizador é autorizado a aceder à rede, sendo marcado com a VLAN apropriada configurada nos **Standard RADIUS attributes**.

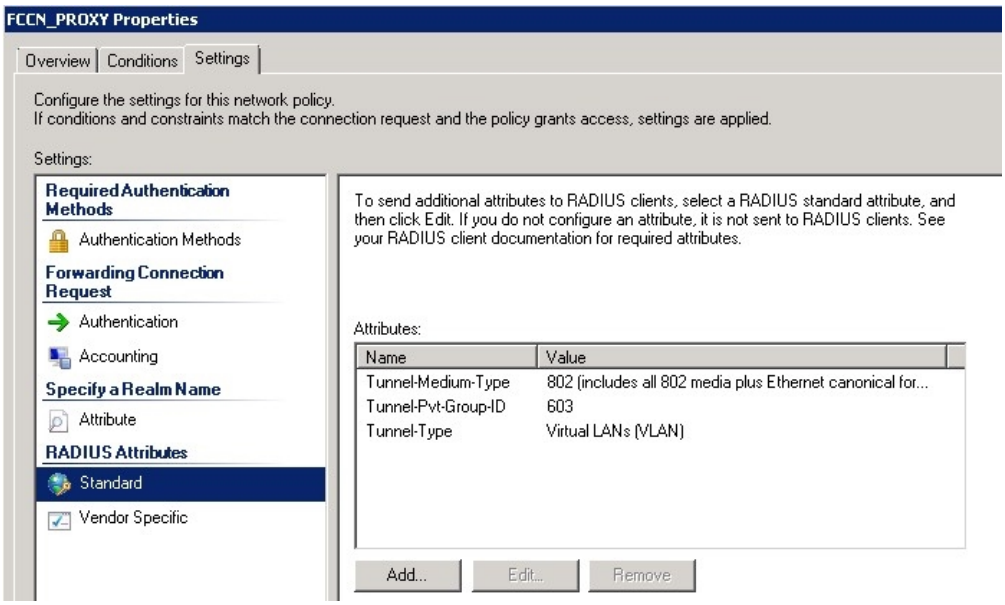


Figura 12: Encaminhamento da informação de accounting

Network Policies

Previamente conhecidas como **Remote Access Policies** no **IAS**, as **Network Policies** distinguem duas componentes, a primeira diz respeito às condições necessárias à aplicação da política, a segunda define o perfil do utilizador, ou seja, as configurações impostas pelo RADIUS para o objeto da autenticação. Exemplifica-se de seguida regra de autenticação de alunos na rede wireless.

Para criar uma nova regra, **RClick** do rato sobre **Network Policies -> New**, e completar com as condições, restrições e configurações de saída. A política de acesso deve ser definida para "**Grant access**" e para que esteja ativa deve ter selecionado o visto "**Policy Enabled**".

Autenticação de alunos internos na rede eduroam

Condições

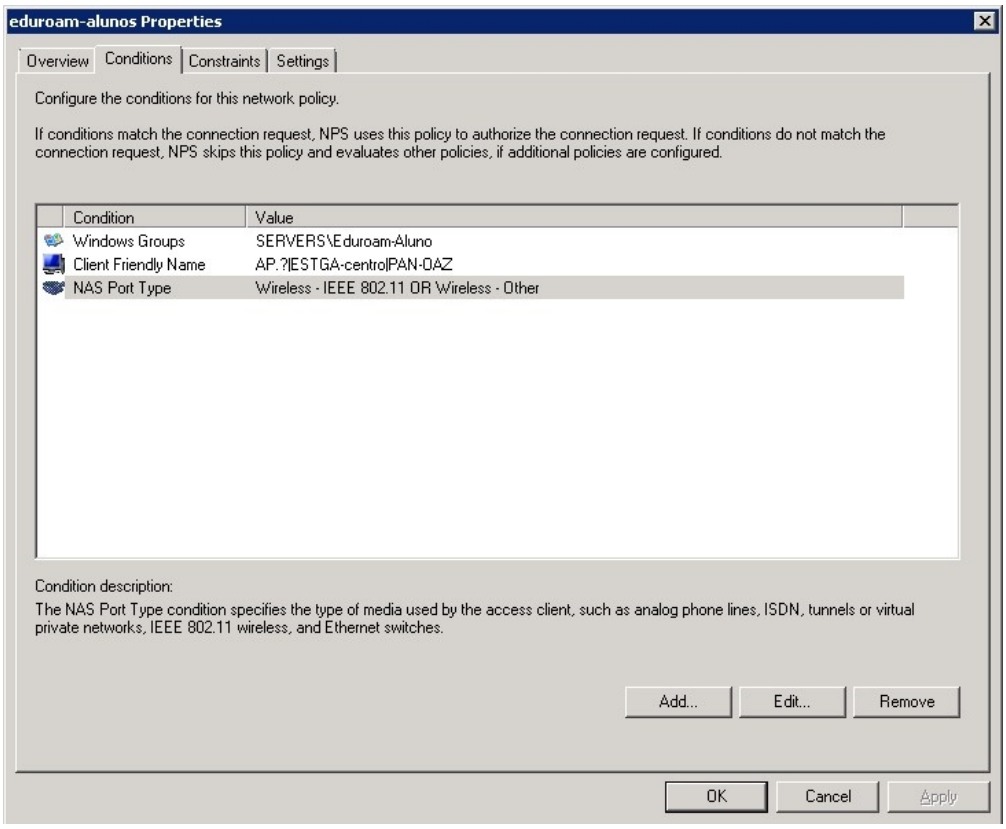


Figura 13: Configuração de condições de acesso

Nesta componente podem ser especificados vários atributos que darão acesso ao perfil. De entre eles, os mais importantes são os que identificam os APs que conferem acesso aos alunos e o grupo LDAP que agrupa o conjunto dos utilizadores que devem ter esse acesso:

- **Client-Friendly-Name**: regexp que identifique todos os APs que conferem acesso à rede eduroam, configurados em **Radius Clients**. (Ex: Se todos os friendly-names dos APs começarem por **AP**, a regexp poderá ser "**AP.?**");
- **Windows-Groups**: Onde se especifica o grupo ou grupos da AD aos quais estão associados os utilizadores com permissões de acesso à rede eduroam.
- **NAS Port Type**: identifica o tipo de meio de transporte. Para autenticação na rede eduroam precisa-se que o meio seja identificado como Wireless.

Restrições

Não são colocadas nenhumas restrições além do método de autenticação. Usamos o método **MS-CHAP v2** dentro de um túnel **TLS** garantido pelo **PEAP**, com validação do certificado do servidor.

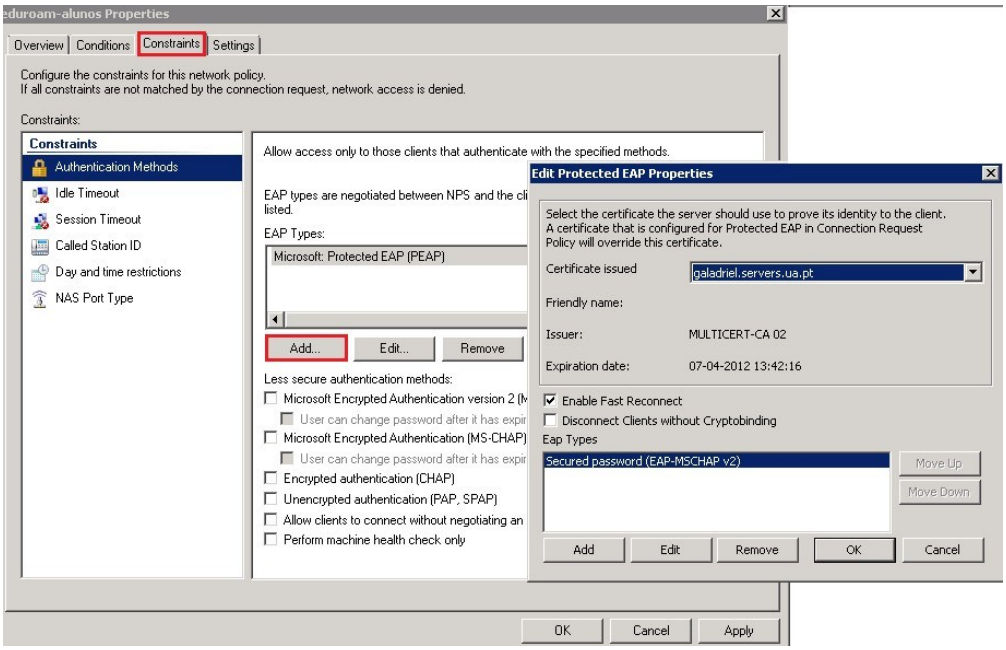


Figura 14: Configuração das Restrições de Autenticação

Para fazer estas configurações, ir ao separador "**Constraints**", na secção de "**Authentication Methods**" fazer "**Add…**" selecionar o protocolo **PEAP**. Se fizermos "**Edit**" é apresentado certificado que o servidor deve usar na comunicação.

Perfil

Se forem cumpridas as condições e as restrições de autenticação, é conferido o acesso e aplicado o perfil. É acessível pelo separador "**Settings**" da regra. Apenas são necessários configurar alguns parâmetros **standard** de funcionamento.

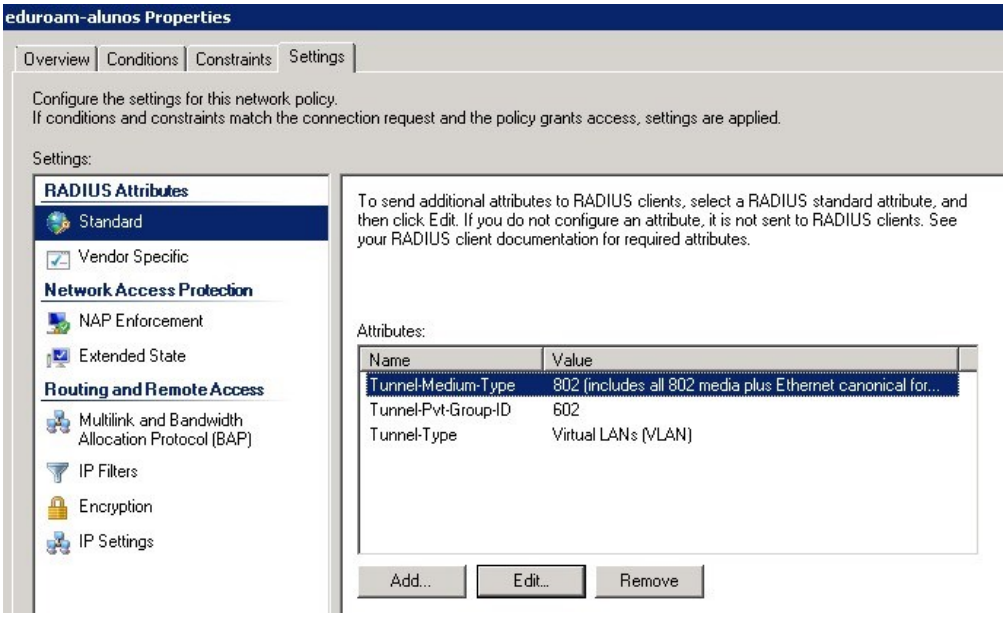


Figura 15: Configuração do Perfil de Utilização

A atribuição de VLANs é feita, através da especificação dos seguintes atributos:

- Tunnel-Medium-Type: **802**
- Tunnel-Pvt-Group-ID: **602** (string com número da VLAN)
- Tunnel-Type: **VLAN**

Aqui podem também ser definidos os VSAs (**Vendor Specific Attribute**) específicos para cada equipamento de acesso à rede.

Nos parâmetros de **Encryption** deve ser configurado o tipo de criptografia apenas para "**Strongest encryption (MPPE 128 bit)**".

Separador Overview

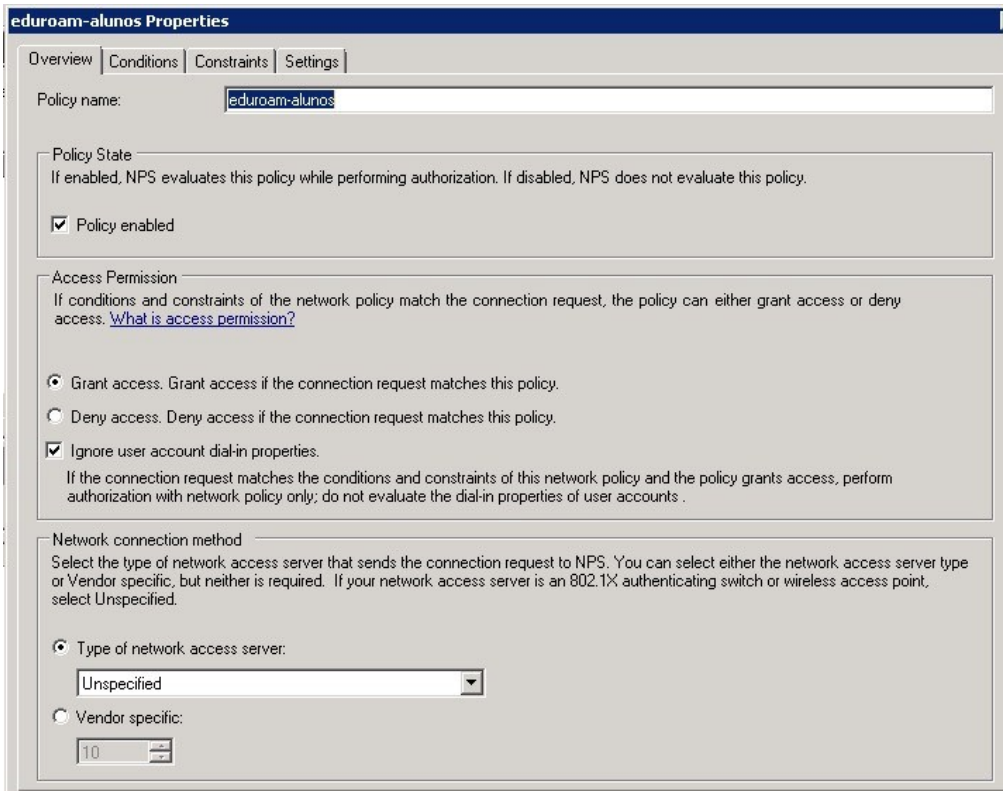


Figura 16: Overview da Network Policy

Depois de criada uma regra, esta pode ser manipulada e visualizada. O separador de **Overview** permite, de forma rápida, (des)ativar a regra, conceder ou negar acesso aos pedidos que coincidem com essa regra e, muito importante, a opção "**Ignore user account dial-in properties**" permite ignorar as propriedades acrescidas dos pedidos, i. e., os atributos e definições adicionais que possam ser incluídas no pedido por parte de quem gerou o pedido (ex: IP pretendido, vlan destino, método de autenticação preferido, etc).

Autenticação de utilizadores internos em Roaming

Configurações que permitem autenticar utilizadores da UA a aceder à rede eduroam noutras instituições.

Para gerir estas autenticações faz-se uso de duas **Network Policies**, a primeira que autentica os pedidos válidos e bem formatados, e outra regra logo de seguida que recolhe os pedidos errados e mal formatados também provenientes dos proxies remotos e ativamente recusa o pedido de autenticação, evitando que estes pedidos sejam ignorados e retransmitidos.

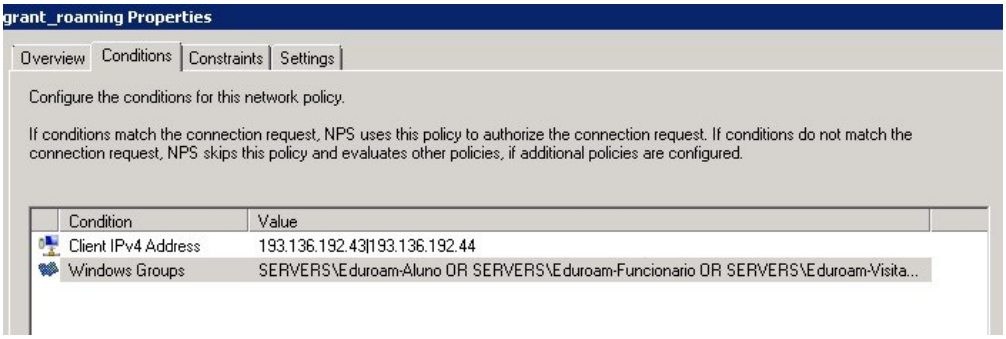


Figura 17: Condições das autenticações de utilizadores internos em roaming

Nas condições de acesso, configuram-se os IPs dos PROXYS da FCCN (clientes desta autenticação). Configuram-se também os grupos LDAP a quem deve ser dado acesso (Windows Groups).

Nota: Em vez de IPs de cliente podem usar-se **friendly names**, usando os nomes empregues na configuração de **RADIUS clients**.

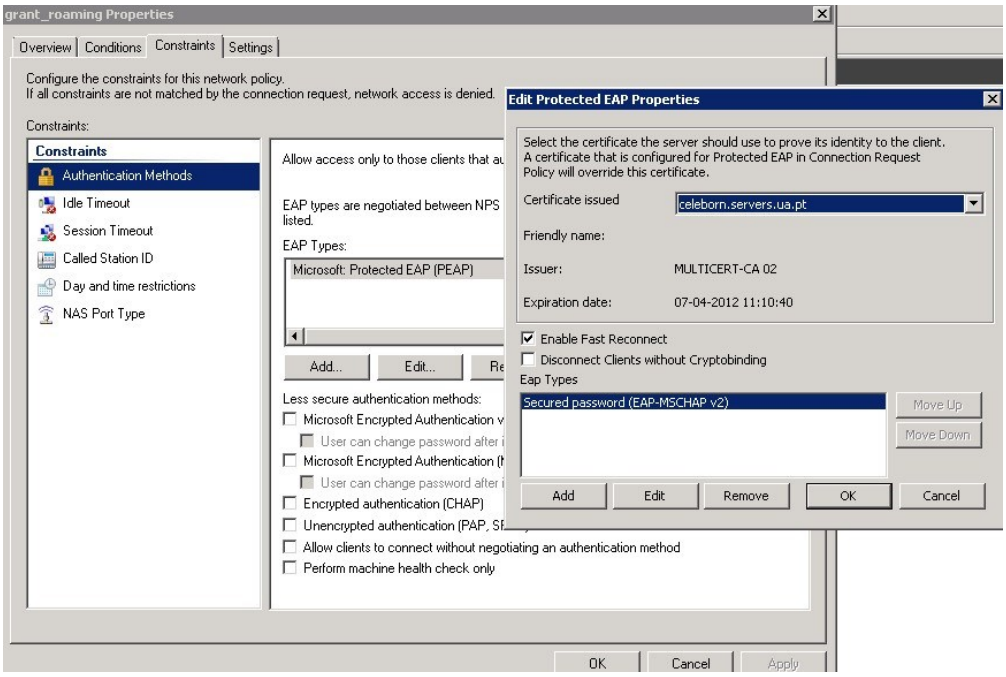


Figura 18: Restrições da autenticação

Nas restrições impõe-se a autenticação PEAP com MSCHAPv2 com a validação de certificado de servidor.

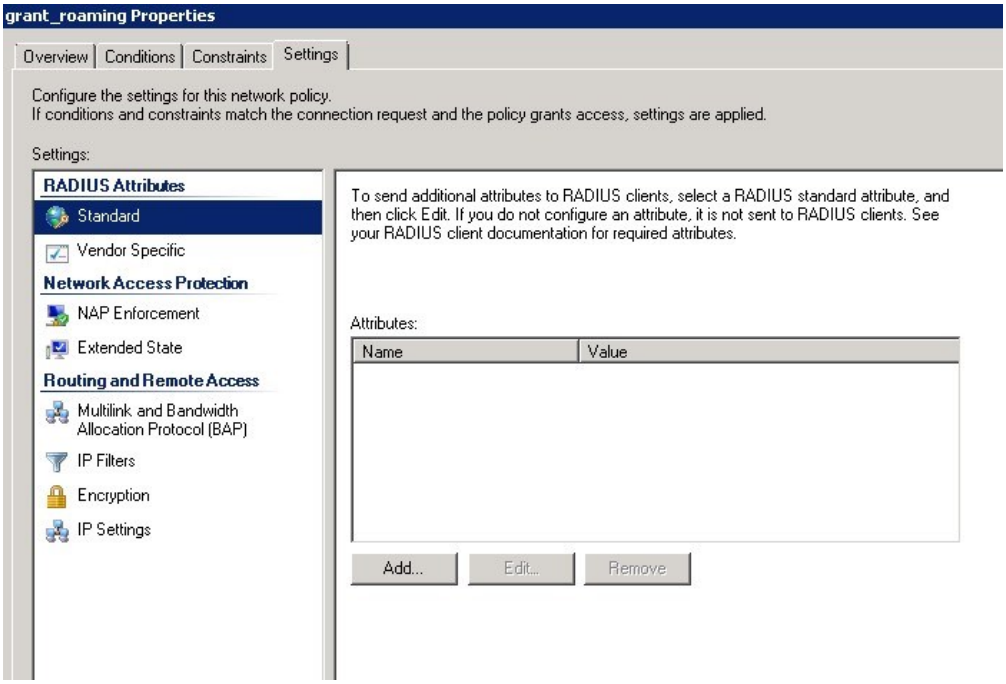


Figura 19: Perfil de saída sem configurações

No perfil de saída não é configurado nada, esta regra serve apenas para autenticar ou não o utilizador. O acondicionamento do utilizador na rede é processado, após validação, no servidor remoto que encaminhou o pedido de autenticação via PROXY da FCCN.

Descarte com resposta dos pedidos mal formatados

Seguida desta regra está aliada uma segunda regra que serve para responder a pedidos mal formatados com negação de acesso (ativa).

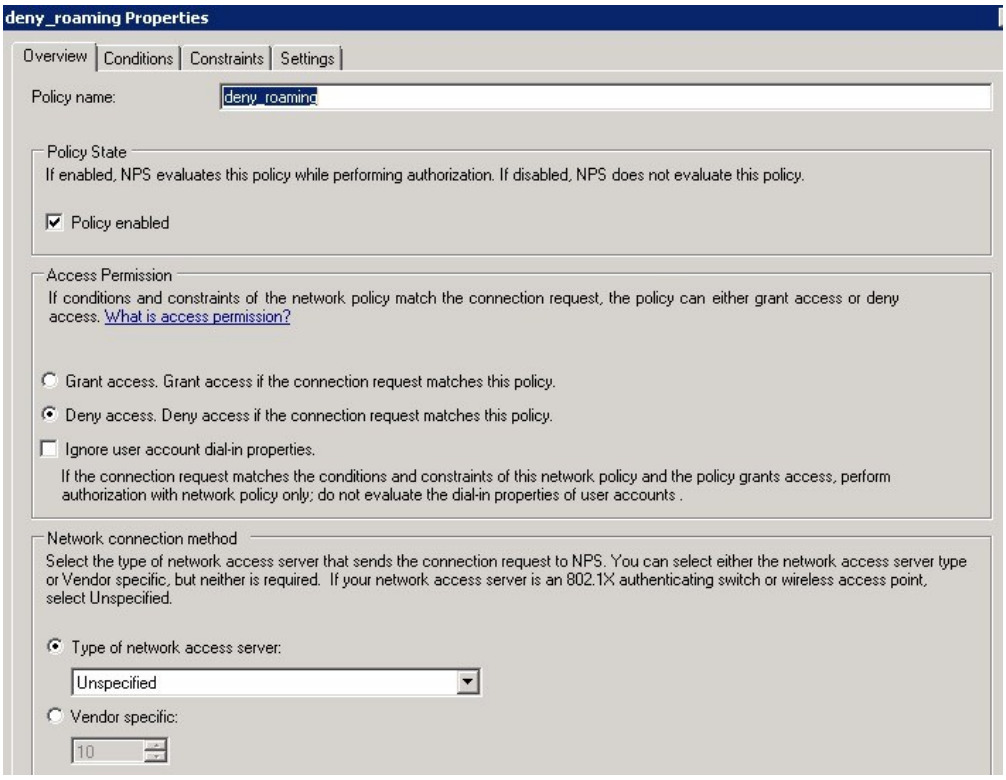


Figura 20: Negação da autenticação

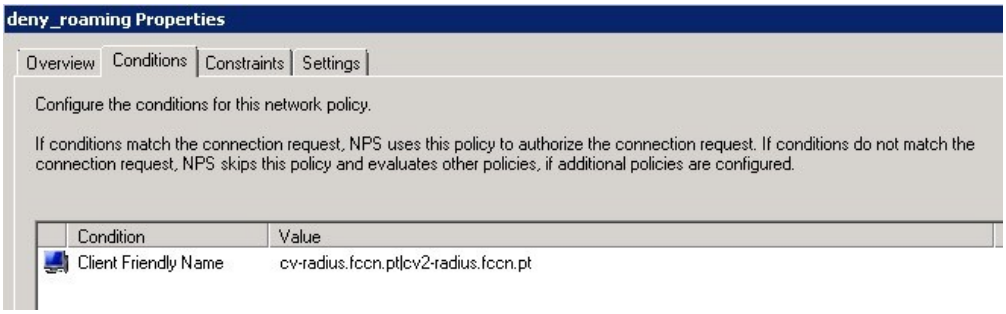


Figura 21: Condição para filtrar os pedidos recebidos da FCCN

Todos os pedidos de autenticação remotos que não cumpram com as condições e restrições da regra de autenticação que valida pedidos fidedignos (regra **grant_roaming** discutida anteriormente), são recolhidos por esta regra e negado o acesso. No separador **overview** é selecionada a opção "**Deny Access**", que negará o acesso a todos os restantes pedidos provenientes do PROXY FCCN. Configuram-se nas condições os **Client Friendly Names** dos proxies da FCCN.

Geração de Certificado de validação do servidor

Para validação do servidor de autenticação por parte do cliente e geração de material criptográfico para a comunicação segura é necessário um certificado de servidor. Em termos gerais, é necessário preencher um formulário genérico, guardado com o formato *.inf, enviá-lo à entidade geradora de certificados, é retornado um certificado que posteriormente se valida e instala no servidor NPS.

Criação do pedido de certificado

Na máquina para a qual se pretende o certificado, cria-se o ficheiro **request.inf** com os dados relevantes seguintes:

Conteúdo do ficheiro para geração de certificado (CSR) chamado **pedido_cert.inf**:

```
[NewRequest]
Subject = "CN = servidor.univ.pt, O = Nome da Universidade, C = PT"
KeySpec = 1
KeyLength = 2048
Exportable = TRUE
MachineKeySet = TRUE
SMIME = False
PrivateKeyArchive = FALSE
UserProtected = FALSE
UseExistingKeySet = FALSE
ProviderName = "Microsoft RSA SChannel Cryptographic Provider"
ProviderType = 12
RequestType = PKCS10
KeyUsage = 0xa0
[EnhancedKeyUsageExtension]
OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication
```

NOTA: Algumas autoridades de certificação de terceiros podem requerer informações adicionais no parâmetro do **Subject**. Essas informações incluem uma unidade organizacional (OU), organização (O), localidade ou cidade (L), país ou região (C) endereço de correio electrónico (E).

O **OID** indica o tipo de certificado que se pretende que seja criado, neste caso para validação de servidor.

Após preenchido o ficheiro e guardado com a extenção ".inf", gera-se o pedido. Na linha de comandos, na pasta onde está o ficheiro request.inf, correr o seguinte comando:

```
certreq -new pedido_cert.inf pedido.req
```

Resulta daqui o ficheiro **pedido.req**. De seguida este ficheiro é enviado à entidade que gera os certificados, que devolverá o certificado pronto a ser instalado.

Aceitação, Instalação e Validação do Certificado

O novo certificado, quando recebido, deve ser assinado com a chave privada residente no servidor onde foi gerado o pedido de certificado. Coloca-se então o certificado.cert recebido na mesma pasta onde foi gerado o pedido e executa-se o comando:

```
certreq -accept certificado.cert
```

Findo este passo, o certificado é assinado com a chave privada e instalado no repositório local de certificados.

No snap-in dos certificados, ao expandir os certificados pessoais do computador local, deve ver-se um novo certificado com objetivo de validação de servidor descrito nas propriedades do mesmo. Este certificado é emitido para o FQDN da máquina. Deve verificar-se a existência dos certificados intermédios e de raiz da cadeia de certificação do certificado em questão. Reiniciar a máquina.

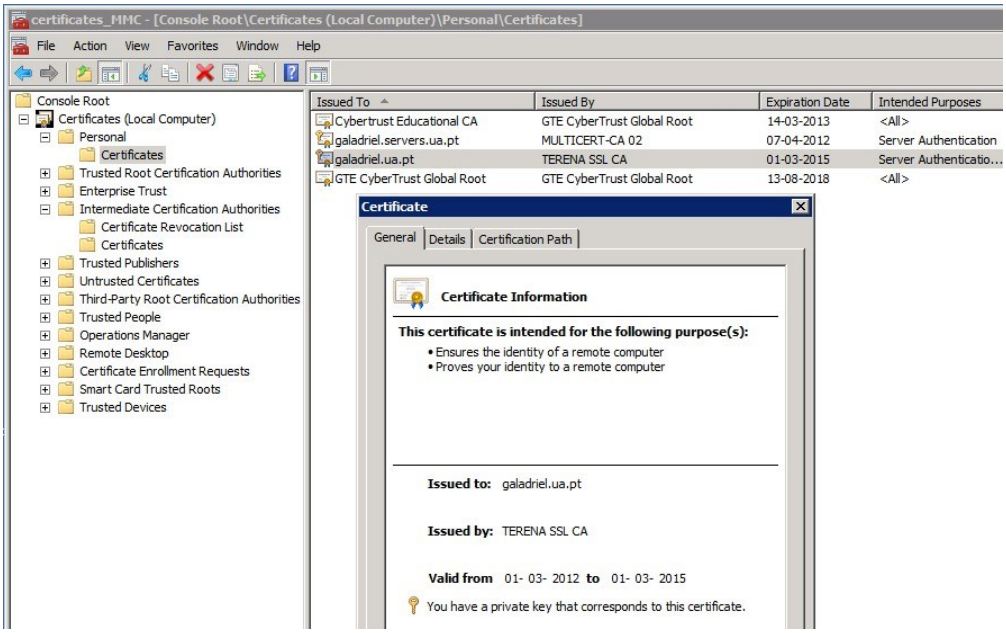


Figura 22: Características do certificado instalado

No link seguinte encontra-se o KB da Microsoft que explica o procedimento de obtenção de um certificado de autenticação de servidor.

http://support.microsoft.com/kb/321051

Anexos

Importação da Base de Dados do IAS para o NPS

Nota: A diferença de arquiteturas impede o upgrade do servidor win2k3 32bit para win2k8(R2)Enterprise uma vez que não é possível atualizar o sistema em 32bit para 64bit.

Considerações

Se o objetivo é manter a estrutura de autenticação tal como existe com o IAS, deve considerar-se o seguinte:

- Os interfaces de rede do novo servidor devem ser configurados nas mesmas redes e com os mesmos IPs, para que não tenham que ser reconfigurados todos os RADIUS clientes para novos encaminhamentos.
- O servidor deve ter o mesmo FQDN para não implicar problemas na importação do certificado de validação do servidor.
- O novo servidor tem que ser registado nos DCs para que a importação da BD valide os “Windows groups” usados na verificação das condições de acesso aquando a autenticação e autorização. Se grupos LDAP relevantes ao NPS são ocultados na AD, devem conceder-se permissões de consulta destes grupos.

Transferência da BD do IAS para o NPS

Para facilitar o processo existe uma ferramenta executável no win2k8 chamada **iasMigReader.exe**, na pasta **C:\Windows\SysWOW64**. Esta ferramenta deve ser copiada e executada no servidor com o IAS. É devolvido um ficheiro, **ias.txt**, alojado na pasta **C:\WINDOWS\system32\ias**.

- Transferir o documento **ias.txt** para o NPS;
- Abrir o NPS e garantir que o serviço está parado e que o servidor está registado na AD:
  - **Action->Stop NPS service**
  - **Action->Register server in Active Directory**
- Importar a BD ao correr o seguinte comando no cmd, na pasta onde for colocado o ficheiro:
  - **netsh nps import ias.txt**

Transferência de Certificado de Validação do Servidor

Mantendo a identidade do RADIUS na rede, o mesmo certificado usado pelo servidor com IAS pode ser usado pelo servidor com NPS. Para tal:

- No IAS:
  - Abrir uma **MMC** (run->mmc) e adicionar um **Snap-in** de **certificates** do **Computer account** para o **Local computer**.

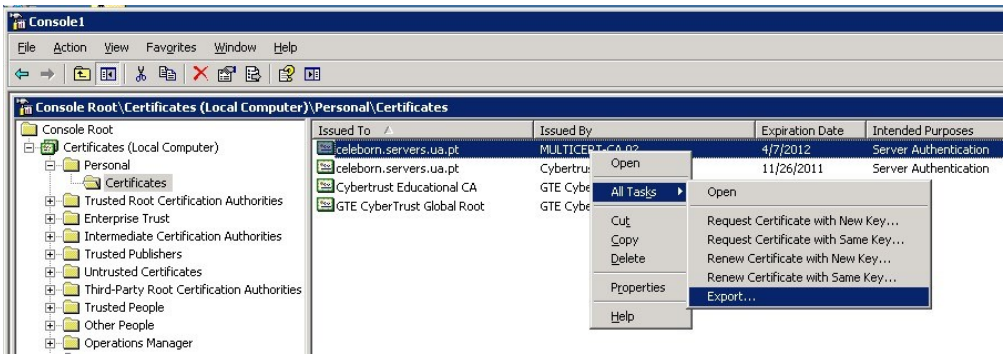


Figura 23: Exportação do certificado do servidor

  - Na pasta **personal -> certificates**, fazer o **export** do certificado de validação do servidor na comunicação EAP. Ao longo do **wizard**, ter atenção em exportar também a chave privada e incluir todos os certificados da cadeia de certificação.
  - É devolvido um ficheiro cifrado com o certificado do servidor.
- No NPS:
  - Na **mmc** de certificados equivalente à do IAS, selecionar a opção de **import** do certificado extraído do IAS. Tal como demonstrado na figura.

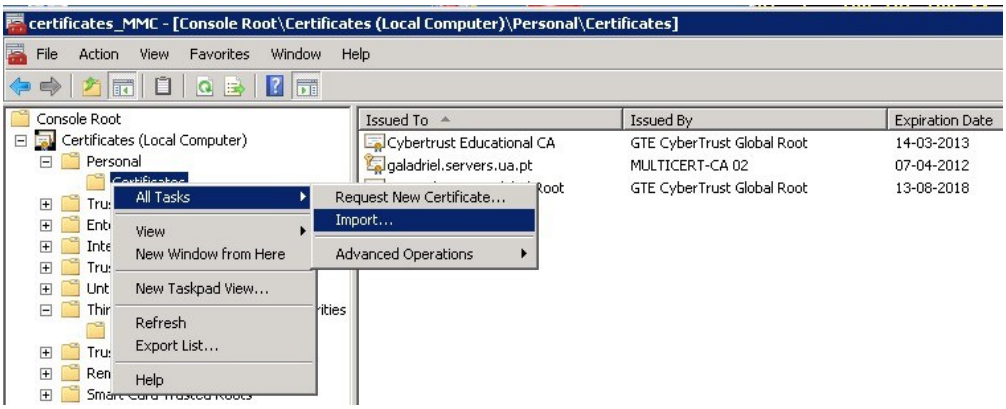


Figura 24: Importação do certificado do servidor

Nota: a opção de exportar o certificado só é necessária no caso de não existir o certificado original para instalação.

Nota: Fazer atenção à cadeia de certificação, podendo ser necessário transferir também certificados de validação intermédia para a pasta "**Intermediate Certification Authorities**".

Nota: Após esta importação do certificado podem existir erros de configurações que impliquem o uso do certificado. Nas configurações das regras (**NPS -> Policies -> Network Policies -> regra_acesso_eduroam**) no separador das **Constraints**, onde se define o método de autenticação, pode ver-se a configuração do PEAP. Se clicar em **Edit**… o erro seguinte aparece:

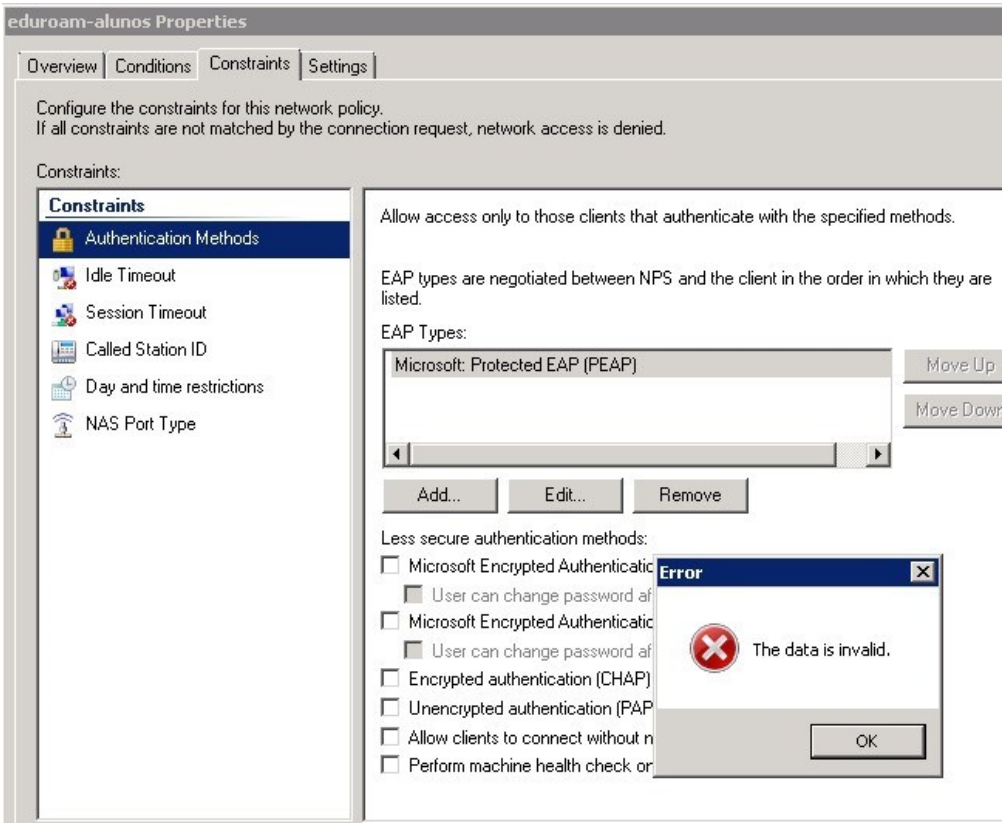


Figura 25: Erro Pós-Import

Assim, para garantir que a autenticação é bem-sucedida, deve voltar a configurar-se este método de autenticação.

- Fazer o Remove do PEAP e selecionar qualquer outro método de autenticação menos seguro para poder aceitar as alterações e sair da janela de configuração;
- Voltar a editar a mesma regra, tirar o visto do método de autenticação menos seguro, fazer **Add**… e selecionar **PEAP**. Se agora for feito o **Edit**… pode ser selecionado agora o certificado de validação do servidor, tal como se mostra a seguir:

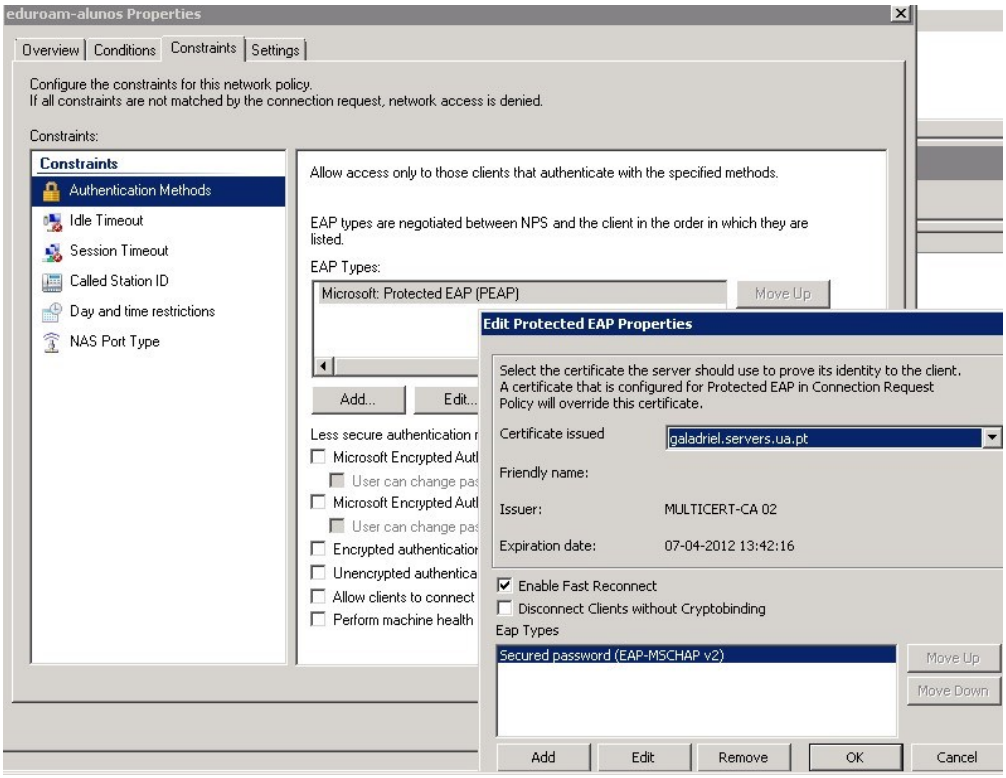


Figura 26: PEAP corretamente configurado após import

A este ponto o servidor RADIUS está pronto a tratar da resposta aos pedidos de autenticação.