Solução eduroam para convidados

Utilização da rede eU/eduroam por utilizadores Convidados

- Utilização da rede eU/eduroam por utilizadores Convidados
- Introdução
  - Objectivos
  - Contributos
  - Enquadramento
- Solução com Realm de Convidados
- Solução com Web Based Login

Introdução

Objectivos

Esta página apresenta uma recomendação técnica para as entidades gestoras da rede eduroam para receber e dar acesso Internet a utilizadores sem credenciais eduroam com recurso à infra-estrutura existente. Esta recomendação visa responder a situações típicas, como a realização de eventos ou reuniões.

Contributos

O presente documento foi disponibilizado à lista de correio electrónico network@e-u.pt, e que comporta a maioria dos administradores dos hotspots e-U, para que a solução apresentada fosse discutida e adicionadas novas contribuições de forma a enriquecer a solução apresentada.

Gostaríamos de agradecer as contribuições e todo o input recebido através dessa lista. Uma palavra de agradecimento especial a:

- Pedro Pinheiro – Univ. Coimbra
- Luís Pisco – Univ. Algarve
- Paulo Valverde Costa – Univ. Minho

Enquadramento

Existem situações em que importa prestar acesso de rede a pessoas que não constam de nenhum servidor de autenticação da rede internacional eduroam. Tipicamente em eventos organizados pelas instituições. Esses utilizadores por não pertencerem a instituições eduroam ficam privados de usar os recursos de rede disponíveis.

Para a maioria dos casos a solução implementada para permitir o acesso à Internet a esses utilizadores passa pela montagem de uma estrutura paralela de hotspot nos locais dos eventos e pela atribuição de contas temporárias. No entanto essa solução obriga à utilização de recursos que nem sempre estão disponíveis e a trabalho adicional.

O ideal será ter a infra-estrutura eduroam preparada para acolher estes novos utilizadores, mantendo os mesmos níveis de segurança e reduzida carga administrativa.

Esta página pretende apresenar uma recomendação para que seja utilizada a infra-estrutura eduroam, de forma contida e controlada, para permitir o acesso à Internet por parte desses “convidados".

Solução com Realm de Convidados

Esta solução é de todas a de mais simples e rápida implementação. A sua instalação aproveita na totalidade a infra-estrutura de acesso e de autenticação existente em cada uma das instituições eduroam.

O seu princípio de funcionamento é em tudo idêntico ao que está implementado na rede eduroam em cada uma das instituições. No entanto os utilizadores autenticam num realm criado especificamente para o efeito. As instituições que queiram implementar este mecanismo devem criar um novo realm nos seus servidores RADIUS do tipo @<instituicao> (por exemplo, a FCCN usa um realm do tipo @fccn – sem o .pt final).
Neste novo realm são criadas um conjunto de contas para atribuição a convidados.

Uma vez que existe a possibilidade destes utilizadores tentarem usar as credenciais indevidamente fora do universo da instituição que lhe atribui a conta temporária irá ser efectuada uma filtragem a nível dos servidores de RADIUS nacionais no sentido de rejeitar tentativas de autenticação que não tenham um TLD associado.

Existe ainda a necessidade de ser efectuada uma gestão criteriosa das credenciais a atribuir. Estas devem ver limitado ao mínimo o seu tempo de vida e deve ser pedido ao seu utilizador que forneça um documento identificativo (tipicamente bilhete de identidade, cartão do cidadão ou passaporte). Relembramos que é responsabilidade da instituição que fornece as credenciais de acesso a um utilizador identificá-lo caso seja necessário.

Tipicamente um utilizador com uma conta de convidado irá configurar o seu equipamento para acesso à rede eduroam disponibilizada pela instituição que o alberga seguindo as indicações disponibilizadas para os demais utilizadores dessa instituição. A sua autenticação será efectuada no mesmo repositório de dados que os utilizadores locais (se assim a instituição o entender) e o acesso à rede serão de acordo com o que está definido para os utilizadores em roaming. Desta forma consegue-se controlar o acesso destes utilizadores a serviços internos das instituições. Em suma, esta solução pressupõe:

- Configuração de um novo realm ‘@<instituição>’ no servidor de autenticação da instituição (exemplo: @fccn);
- Filtragem central de todos os pedidos de roaming que não tenham associado um TLD válido;
- Criação de um bloco adequado de credenciais;
- Gestão desse bloco de credenciais, incluindo rotação mensal;
- Registo da atribuição das credenciais aos utilizadores para efeito de auditagem.

Solução com Web Based Login

Uma segunda solução possível assenta numa plataforma de autenticação Web Base. Esta é a solução mais trabalhosa a nível de implementação e de manutenção.

Em termos de serviços, esta solução necessita que sejam instalados os servidores de autenticação e HTTP.

É ainda necessário que sejam configurados e geridos o(s) SSID(s) onde o serviço vai ser prestado. Podem ser usados os access points que estão actualmente instalados e a dar acesso à rede eduroam. No entanto devem ser tomadas todas as medidas que permitam distinguir este serviço do serviço eduroam, nomeadamente é expressamente interdita a presença de referências à rede eduroam nas páginas de autenticação ou em qualquer lugar visível nesse servidor Web.

Devem ainda ser tomado em consideração que este novo SSID e este novo método de autenticação não devem de modo algum gerar qualquer impacto ou degradação no serviço eduroam em produção.