Uma Plataforma para Gestão de Configurações em Redes de Banda Larga

T. Leite[1], P. Simões[1], T. Cruz[1], F. Bastos[2], E. Monteiro[1]

[1]CISUC – Dep. Eng. Informática, Universidade de Coimbra
E-mail: thiago@student.dei.uc.pt, {psimoes, tjcruz, edmundo}@dei.uc.pt

[2]Portugal Telecom Inovação
E-mail: fbastos@ptinovacao.pt

***Resumo*— Este artigo apresenta uma plataforma de gestão de perfis e configurações concebida na óptica do operador, para gestão remota do cadastro e das configurações de dispositivos de redes domésticas de banda larga fornecidos pelo operador (*routers* domésticos, telefones VoIP, *set-top-boxes*, etc.). A plataforma proposta inclui mecanismos bastante flexíveis de administração, de modo a suportar a grande diversidade de equipamentos e serviços típica destes ambientes. A plataforma permite também incorporar no processo os perfis dos utilizadores (serviços contratados, perfil típico de uso, etc.), de modo a assegurar um processo de gestão de configurações mais eficiente.**

***Keywords*— Gestão de Redes, Gestão de Configurações, Redes de Acesso de Banda Larga.**

I. Introdução

A tendência que se tem vindo a registar no sentido de fazer convergir digitalmente diversos serviços num único canal de comunicação, adoptando para o efeito o protocolo IP (*Internet Protocol*), aliada ao acréscimo de capacidade e qualidade de serviço proporcionado pelas redes de acesso de banda larga, possibilitou aos operadores de acesso (*Service Provider*) oferecer novos serviços de valor acrescentado, tais como voz, televisão, *video-on-demand* e televigilância. No entanto, esta evolução acarreta um desafio relevante: enquanto anteriormente o operador de acesso se preocupava apenas em oferecer conectividade, terminando a sua responsabilidade no *modem* do cliente, hoje em dia ele acaba por ser directa ou indirectamente responsável por uma parafernália de dispositivos por si fornecidos ao cliente (*routers* domésticos, *set-top-boxes*, centrais de alarme, *webcams*, equipamentos *powerlan*, etc.) sem os quais serviços essenciais como o telefone ou a TV deixam de funcionar.

No âmbito do Projecto S3P [1], foi concebida e implementada uma plataforma de gestão para redes de acesso de banda larga, tendo por paradigma a cooperação activa entre o operador e as diversas redes domésticas servidas pela rede de acesso. Ainda que o principal objectivo deste projecto fosse a segurança (construindo-se para o efeito um sistema fortemente distribuído de detecção e prevenção de intrusões), a plataforma acaba por ser útil também para a gestão remota de configurações de todo o tipo de equipamentos fornecidos ao operador para instalação nas redes domésticas dos clientes de banda larga (CPE: *Customer Premises Equipment*).

Neste artigo descreve-se precisamente a vertente de gestão de configurações associada à plataforma S3P. Ainda que os objectivos iniciais fossem apenas dar suporte à gestão de segurança, as suas funcionalidades são suficientes para que possa ser usada, autonomamente, como plataforma de gestão de configurações de CPE.

O resto deste artigo encontra-se organizado da seguinte forma: a Secção II discute trabalho relacionado. A Secção III faz alguma contextualização, em termos de motivação e de enquadramento no projecto S3P. A Secção IV apresenta a plataforma de gestão de configurações, e a Secção V discute questões de implementação. A Secção VI conclui o artigo.

II. Revisão do Estado da Arte

II.A Normalização

A necessidade de integração dos CPE na infraestrutura de gestão das redes de acesso de banda larga é largamente reconhecida pela indústria. Nesse sentido, não é de admirar que sejam dois *Fora* industriais a assumir as actividades mais visíveis nesta área: a HGI (*Home Gateway Initiative* [2]) e, actualmente com maior expressão, o *Broadband Forum* [3]. Ambas as iniciativas assumem, para além de objectivos mais alargados de normalização e disseminação de serviços e tecnologias de banda larga, a preocupação com a gestão remota de CPE.

As especificações da próxima geração de CPE, definidas pelo HGI, incluem mecanismos de administração remota dos equipamentos por parte dos operadores de serviço, prevendo que essa gestão inclua não apenas os CPE fornecidos pelo operador mas também outros dispositivos instalados pelo cliente, tais como computadores domésticos ou televisores compatíveis. No entanto, estas especificações estão ainda longe de ser uma norma de *facto* promovida de modo alargado por fabricantes de acesso.

O trabalho desenvolvido pelo *Broadband Forum* (conhecido anteriormente por *DSL Forum*), cujos objectivos são parcialmente sobrepostos com os da HGI, inclui uma proposta mais completa para administração remota de CPE, sendo especialmente relevante a especificação técnica TR-069 [5], um protocolo para gestão de CPE através de redes de acesso (também conhecido como CWMP: *CPE WAN Management Protocol*). O TR-069 e o conjunto de normas que agrupa definem uma camada de aplicação segura para a gestão remota de CPE a partir de aplicações instaladas no operador de

serviço que conhece uma aceitação crescente e é já suportada por alguns dos dispositivos domésticos actuais.

II.B Soluções Comerciais

Actualmente continuam a prevalecer as soluções proprietárias para gestão de CPE, com base na modificação dos CPE fornecidos pelos fabricantes (i.e., customizando o *firmware* desses dispositivos à medida das necessidades do operador) e no uso de mecanismos proprietários para forçar operações básicas como a actualização remota de *firmware*. Estas soluções acabam por exigir um esforço de manutenção considerável (é necessário modificar o *firmware* de todos os CPE fornecidos, por vezes de modelos e fabricantes diferentes, e é difícil aproveitar de forma simples as actualizações genéricas de *firmware* fornecidas pelos próprios fabricantes) e são frequentemente limitadas em termos de segurança e/ou funcionalidades. Como exemplo de solução proprietária podem mencionar-se, por exemplo, os produtos da *iPass* [6].

Começam também a surgir algumas soluções baseadas no TR-069, desonerando os operadores de serviço de todo o esforço de manutenção associado a esquemas proprietários. Destacando-se, a esse nível, quatro soluções: *Axiros* [6], *Gatespace* [7], *Works Systems* [9] e *Dimark* [10]. A tabela I resume a oferta analisada no contexto deste artigo.

Tabela I - Soluções para a gestão de configurações.

Principais soluções comerciais para gestão de CPE	
Axiros	*Appliance* integrado utilizando TR-069 para gestão de CPE
Gatespace	Desenvolvimento do TR-069 e do servidor do lado do operador de serviço
Work Systems	*Appliance* integrado utilizando TR-069 para gestão de CPE
Dimark	Agente TR-069 portado para várias plataformas de CPE
iPass	Solução proprietária para monitorização e gestão de CPE próprios

III. PROJECTO S3P

Como resposta à crescente dificuldade em escalar soluções de segurança clássicas do lado do operador, o Projecto S3P propõe um modelo de segurança distribuído, que faz uso das capacidades de processamento e gestão remota dos *routers* domésticos para transferir parte dos mecanismos de segurança para os CPEs. Considerando o razoável poder computacional existente nos actuais *routers* de banda larga, assim como a posição privilegiada que estes ocupam ao nível da rede de acesso (na fronteira entre o operador de serviço e o cliente), pode-se considerar que, sem custos adicionais, é possível ampliar as funções por eles desempenhadas, por via da incorporação de meios de detecção e prevenção de ataques, além da geração de estatísticas personalizadas de uso do ambiente (padrões de utilização, eventos de segurança mais relevantes no contexto do operador). Estas informações podem ser correlacionadas de modo a detectar eventos de segurança de modo eficiente [11] e assim permitir que o sistema de detecção de intrusão do operador de serviço possa controlar remotamente a configuração dos diversos *routers* domésticos, de modo a activar configurações que permitam mitigar e/ou prevenir riscos de segurança para os clientes, para o próprio operador de serviço ou para terceiros. Uma descrição mais detalhada da plataforma S3P está disponível em [1][12].

Um dos componentes fundamentais do paradigma de funcionamento associado à plataforma S3P é o facto de todas as acções de segurança, sejam elas correctivas ou preventivas e accionadas a nível local (por decisão autónoma do CPE) ou global (por decisão do operador de serviço) se traduzirem, na prática, por modificações de configurações dos CPE. Estas modificações poderão corresponder à instalação ou actualização de componentes de software nos CPE (i) e/ou à modificação das parametrizações destes componentes de software (ii). Como exemplo do primeiro caso podemos mencionar a actualização da versão da *firewall* instalada no CPE, e como exemplo do segundo caso podemos mencionar a modificação das regras de funcionamento dessa mesma *firewall*, passando a bloquear determinado porto.

Facilmente se compreende que, neste contexto, é fundamental ter um mecanismo que permite accionar remotamente actualizações de configuração e, em paralelo, manter ao nível do operador de serviço uma relação com as configurações activas em cada CPE.

A gestão de configurações de CPE por parte do operador de serviço é porem uma tarefa complexa, pelo factor de escala (mesmo considerando um único CPE por cliente estarão em causa milhares ou milhões de dispositivos) e, acima de tudo, pela diversidade. Esta diversidade reflecte-se em várias dimensões: diversos tipos de dispositivos (*routers*, telefones VoIP, centrais de vigilância e domótica, *set-top-boxes*, etc.), diversos modelos para cada tipo de dispositivo (por exemplo *routers* de fabricantes e modelos diversos), e perfis distintos de cliente para cliente (serviços contratados, tipo de cliente, etc.). Do ponto de vista de funcionalidades seria desejável tratar diferenciadamente cada CPE, como um caso específico, enquanto do ponto de vista de custos de operação seria desejável tratar todos os CPE de forma uniforme.

Ainda que seja obviamente impossível satisfazer simultaneamente estes dois desejos, a solução proposta para gestão de configurações de CPE no contexto do Projecto S3P, tenta conciliar as duas perspectivas, oferecendo mecanismos de diferenciação que dêem suporte à natural diversidade de clientes e equipamentos, mas mantendo em paralelo ferramentas de automação e uniformização que contenham os custos operacionais. Na próxima Secção serão descritas as principais características dessa plataforma.

IV. PLATAFORMA DE GESTÃO DE CONFIGURAÇÕES

A solução de gestão de configurações de CPEs do Projecto S3P, que designaremos por *Configuration Manager*, é composta por elementos integrados no próprio CPE e por elementos integrados na plataforma de administração do operador de serviço.

O *Configuration Manager* é flexível relativamente às tecnologias de comunicação entre o CPE e a plataforma do operador de serviço. Ainda que preconize o uso do já mencionado protocolo TR-069 como mecanismo preferencial de comunicação entre o operador de serviço e o CPE (e que tenha sido essa a solução adoptada na implementação do

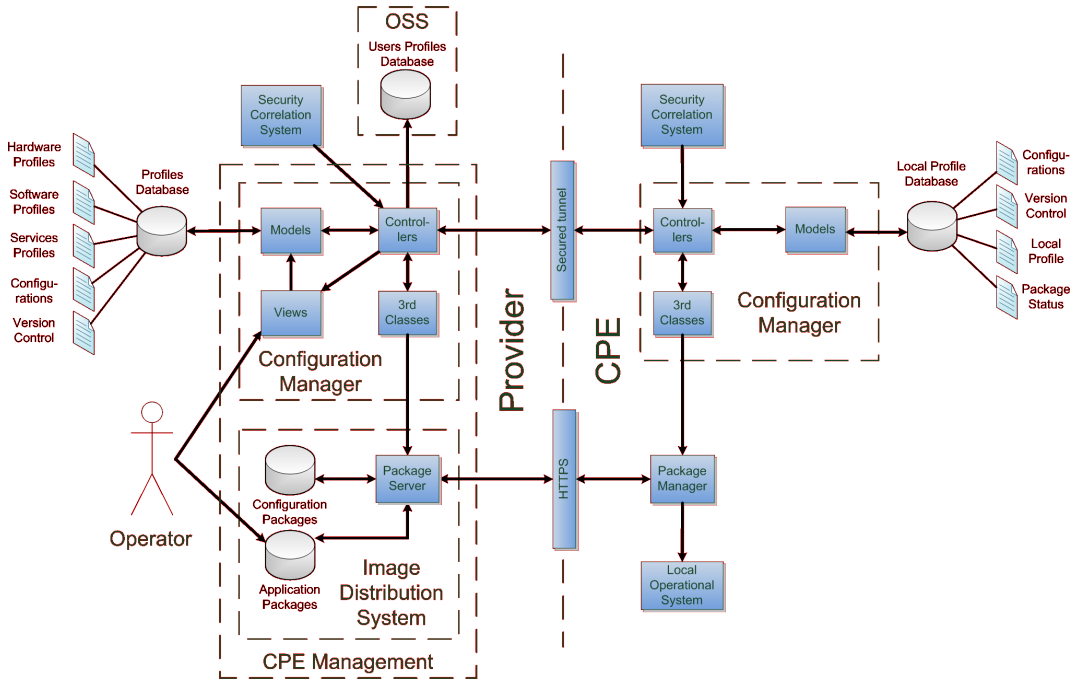

Fig. 1. Arquitectura geral do *Configuration Manager*.

protótipo), poderão ser igualmente utilizadas soluções alternativas quando os CPEs não suportem TR-069 (por exemplo *webservices* genéricos ou soluções proprietárias baseada em *sockets* seguros). Em complemento ao TR-069, usado como interface de monitorização e controlo, a transferência de ficheiros do operador de serviço para o CPE (pacotes com software e/ou com configurações) é feita por HTTPS, em linha com as recomendações do *Broadband Forum*.

A Fig. 1 apresenta os principais elementos desta solução. Segue-se a descrição dos principais componentes da arquitectura, organizada de acordo com a sua localização.

a) Componentes Integrados na Plataforma do operador de serviço

O ***Configuration Manager*** (Fig. 2) é o componente principal da arquitectura, sendo responsável por correlacionar perfis e criar configurações, além de assegurar a comunicação com os CPE por meio do protocolo TR-069 (monitorização, pedidos de actualização de configurações, etc.). Este módulo mantém uma base de dados bastante completa com as configurações instaladas em cada CPE (software e parametrizações, conforme foi já discutido), as características de hardware desse CPE, os perfis do cliente onde se encontra instalado esse CPE (incluindo os serviços contratados) e o histórico de actualizações nesse CPE.

O *Configuration Manager* mantém também uma relação de compatibilidades e interdependências (hardware, software, ficheiros com parametrizações, perfis de cliente) de modo a poder determinar quais as configurações adequadas para cada componente de cada CPE. As possibilidades de correlação entre perfis são inúmeras e dependem do contexto: certos serviços podem ser associados a modelos de CPE; grupos de utilizadores de uma cidade podem ser associados a um ou vários perfis comuns de software; uma versão específica da configuração de um componente pode ser associada a um conjunto de versões binárias desse componente, etc. A possibilidade de existência de relações com diferentes graus de cardinalidade, como será o caso de um perfil associado a vários outros, exige que este componente seja flexível no sentido de acomodar as combinações possíveis.

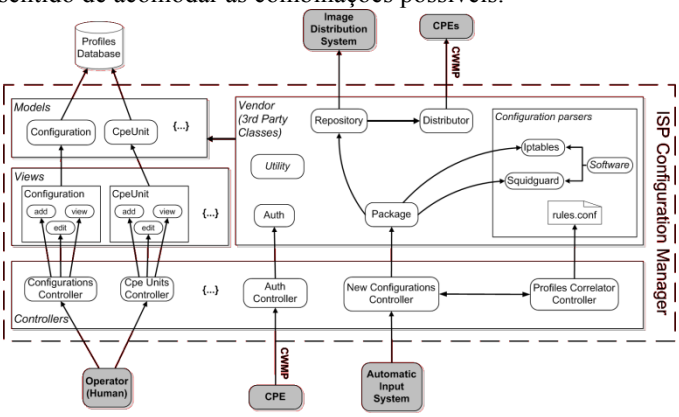

Fig. 2. *Configuration Manager* (do lado do operador de serviço).

O operador de serviço pode ordenar ao CPE uma actualização de componentes ou de parametrizações em dois cenários distintos.

Um desses cenários corresponde à definição, por parte de técnicos da equipa de administração do operador de serviço, de uma nova regra automática de actualizações que afecte o CPE em questão (por exemplo uma regra que indica que todos os CPE de dado modelo e com utilizadores com o perfil P deverão actualizar a sua firewall para a versão *x.y*). Nesse caso o CPE é notificado para transferir os ficheiros em questão (previamente criados e armazenados pelo operador de sistemas) e proceder à actualização.

O segundo cenário relaciona-se com os componentes de detecção e intrusão da plataforma S3P (*Security Correlation System*, na Fig. 1). Quando estes componentes decidem reagir a uma determinada situação de risco poderão criar

automaticamente novas regras para determinados CPE. As regras assim criadas poderão ser estáticas (por exemplo instalar uma parametrização previamente armazenada, de modo manual, pelo operador de sistemas) ou dinâmicas (por exemplo adicionar à configuração actual da firewall o bloqueio de dois portos específicos). Neste último caso é possível recorrer a *configuration parsers* (por meio do *New Configuration Controller*, vide Fig. 2) com capacidade de interpretar e modificar as parametrizações activas, gerando assim novas parametrizações. Foram até ao momento implementados *configuration parsers* para as duas principais barreiras de segurança do CPE: *iptables* (*firewall* [13]) e *squidguard* (filtro de conteúdos *Web* [14]).

A Fig. 3 apresenta o Diagrama de Fluxo de Dados (DFD) para a criação de uma auto-configuração desde o momento que a regra é enviada pelo sistema de correlação de eventos de segurança e recebida pelo *New Configurations Controller* até ser instalada nos clientes.

Através do módulo *Auth Controller* (vide Fig. 2) é possível que os CPEs possam autenticar e registar-se no *Configuration Manager*, actualizando assim dados ou atributos que tenham sido entretanto modificados, como o endereço IP.

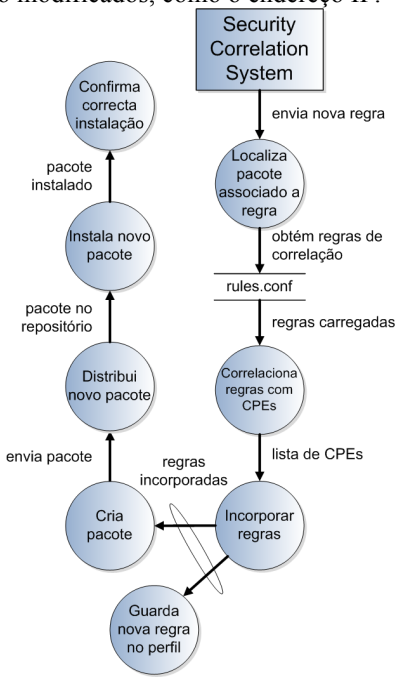

Fig. 3. DFD da auto-configuração dos CPEs.

O segundo componente do lado do operador de serviço é o ***Image Distribution System***, responsável pelo armazenamento e distribuição dos ficheiros com novas versões (software, configurações) para os CPE. Estas novas versões podem ser criadas *off-line* pelos técnicos de administração do operador de serviço (que se limitarão posteriormente a importar os ficheiros correspondentes para a base de dados do *Image Distribution System*) ou, em alternativa, poderão corresponder a parametrizações dinâmicas criadas pelos já mencionados *configuration parsers*. Deste modo, poderão coexistir configurações bastante genéricas e criadas manualmente com configurações muito específicas (no limite para um único CPE), criadas dinamicamente pela própria plataforma, em resposta a riscos de segurança.

Um outro aspecto importante prende-se com a gestão de versões: conforme a configuração dos CPE vai sendo alterada, e visto o mesmo CPE poder estar associado a diferentes perfis de acordo com os serviços subscritos, irá adquirindo determinadas especificidades ao longo do tempo. Tal facto justifica a necessidade de manter diferentes versões de configurações para cada CPE (ou conjunto de CPE). Os CPEs são identificados de acordo com o número de série, o que permite referenciá-los unicamente perante os demais. Na prática cada dispositivo têm um histórico de configurações no operador que dá suporte a operações de *debugging* e *rollback*.

A principal diferença entre um sistema comum de distribuição e armazenamento de pacotes e o *Image Distribution System* é a organização dos pacotes, que são separados conforme correspondam a configurações ou binários executáveis. Os componentes e módulos dos serviços são divididos em pacotes binários e/ou um ou vários pacotes de configuração, de modo a que seja possível ao operador de serviço ter diferentes parametrizações para um mesmo módulo/serviço. O *Image Distribution System* é baseado na ferramenta *opensource* Apt (*Advanced Package Tool* [15]), tirando assim partido de uma estrutura de distribuição de configurações e componentes já desenvolvida e que se tem revelado segura e fiável.

b) Componentes no lado do CPE

A Fig. 4 apresenta os componentes do ***Configuration Manager*** instalado em cada CPE.

Uma das diferenças relativamente ao serviço homónimo do operador de serviço reside na forma como são desencadeadas as operações de actualização. Enquanto no operador de serviço essas operação são provocadas por acções do operador de sistemas ou dos módulos de segurança (correlação de eventos de segurança ao nível do operador), as acções de reconfiguração decididas autonomamente pelo CPE são despoletadas unicamente pelo módulo de segurança local (que reage a riscos de segurança detectados localmente), ilustrado na Fig. 4 como *Automatic Input System*.

A outra diferença reside no facto de deixar de ser necessário manter uma base de dados tão completa de perfis, equipamentos e interdependências, dado que esse controlo é feito ao nível do operador de serviço. A base de dados do CPE fica assim substancialmente simplificada, mantendo apenas a informação suficiente para que as configurações mantidas localmente sejam adequadamente processadas.

Assim como no operador de serviço, os controladores constituem a interface para a entrada de dados externos, como as modificações de dados persistentes ou mesmo as ordens enviadas pelo operador de serviço. O *Configuration Manager* do lado do cliente possui dois controladores: *New Configurations Controller* e *System Controller*.

O New Configurations Controller do CPE possui uma função semelhante à do controlador análogo existente no operador de serviço, sendo encarregado de tratar os pedidos locais gerados pelo sistema automatizado de entrada de dados para criar dinamicamente novas configurações. Tal como no caso do operador de serviço, actualmente este módulo suporta as aplicações *Iptables* e *Squidguard*.

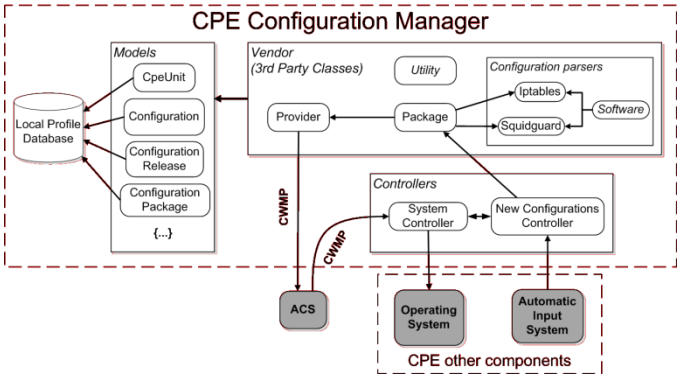

Fig. 4. Configuration Manager (do lado do CPE).

Através do *System Controller* é possível ao operador de serviço enviar ordens para que o CPE actualize seu sistema, instale determinado componente ou apenas verifique se as definições do repositório estão correctamente configuradas.

Um outro componente residente no CPE é o *Package Manager*, responsável pela obtenção de pacotes junto do *Image Distribution System* do operador de serviço e pela sua manutenção a nível local.

V. Protótipo e Casos de Uso

Para a validação da solução proposta foi implementado um protótipo completamente funcional, enquadrado na Plataforma S3P. Esse protótipo foi posteriormente instalado no Piloto AMORA (uma rede experimental de banda larga, com serviços *Triple Play*, mantida pela PT Inovação em Aveiro).

No protótipo o módulo denominado genericamente na arquitectura como *Automatic Input System* corresponde ao motor de correlação de eventos de segurança da plataforma S3P. Este motor de correlação, que funciona a dois níveis, pode solicitar a inserção automática de pedidos de criação de auto-configurações, tanto ao nível local (CPE) como ao nível global (operador de serviço).

São de seguida discutidos três dos casos de uso representativos que foram testados com sucesso no referido protótipo:

- Entrada manual de novas configurações, por parte do operador de sistemas, e posterior distribuição pelos clientes.
- Entrada automatizada de pedidos de reconfigurações dinâmicas, a pedido do sistema de correlação de eventos de segurança que funciona no operador de serviço.
- Entrada automatizada de pedidos de reconfigurações dinâmicas, a pedido do sistema de correlação de eventos de segurança que funciona no CPE.

A. Entrada manual de novas configurações

O operador humano é um actor fundamental neste caso de uso. É através dele que as configurações são manualmente criadas e armazenadas no operador de serviço, sendo também ele que modifica os perfis do sistema de modo a associar essas configurações a determinados CPE. As configurações manualmente criadas pelo operador constituem pacotes que podem ser distribuídos a um conjunto de CPEs associados a algum perfil específico.

A partir do momento em que o operador cria uma nova configuração, esta é associada com uma versão e um perfil (passos 1 e 2 ilustrados na Fig. 5), sendo os dados distribuídos aos clientes. As configurações criadas pelo operador são estáticas, sendo possível associá-las com diversos CPEs. Um pacote é disponibilizado no repositório para todos os clientes que forem associados a esses perfis (3). O *Configuration Manager* do operador de serviço envia a ordem ao *Configuration Manager* de cada CPE (por meio do TR-069) para que estes instalem o novo pacote (passos 4 e 5). São também são enviadas instruções aos CPEs sobre o novo pacote que para estes sejam armazenados localmente (6). Após ter sido realizada a instalação do pacote (7) verifica-se se este foi correctamente instalado e procede-se à actualização da informação na base de dados central do operador de serviço e na base de dados local do CPE (8).

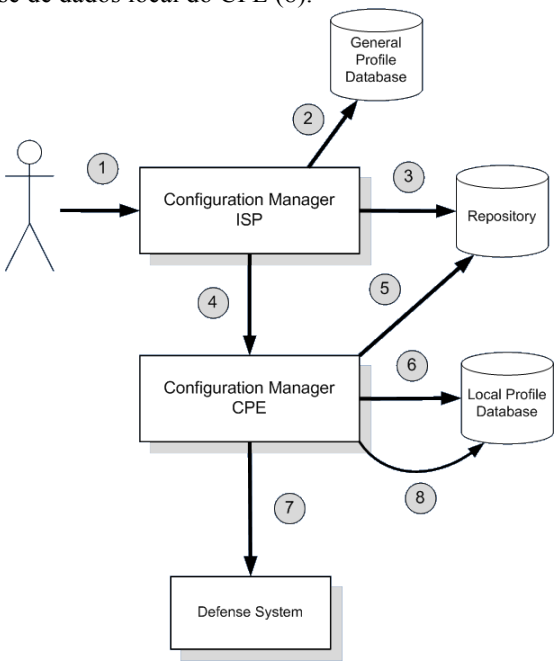

Fig. 5. Caso de uso do operador inserindo novas configurações.

B. Entrada automatizada de dados no operador de serviço

O segundo caso de uso, ilustrado na Fig. 6, corresponde à entrada de uma ordem de actualização dinâmica de parametrizações, emitida pelo sistema de correlação de eventos de segurança do operador de serviço.

Neste caso concreto um determinado porto TCP/IP passou a ser considerado inseguro para um conjunto de CPEs, devido a um elevado índice de eventos de segurança directamente relacionados com esse porto. O motor de correlação de segurança ordena a inserção de uma regra na *firewall Iptables* dos CPE vulneráveis para bloqueio do porto (1). O *Configuration Manager* recebe e processa esta ordem (usando o *configuration parser* para gerar uma nova configuração) e, a partir dela, correlaciona com os CPEs que receberão a nova configuração (2). Cria então novas configurações personalizadas para cada CPE e inclui no repositório de pacotes essas novas configurações (3). Os demais passos seguem o caso de uso anterior.

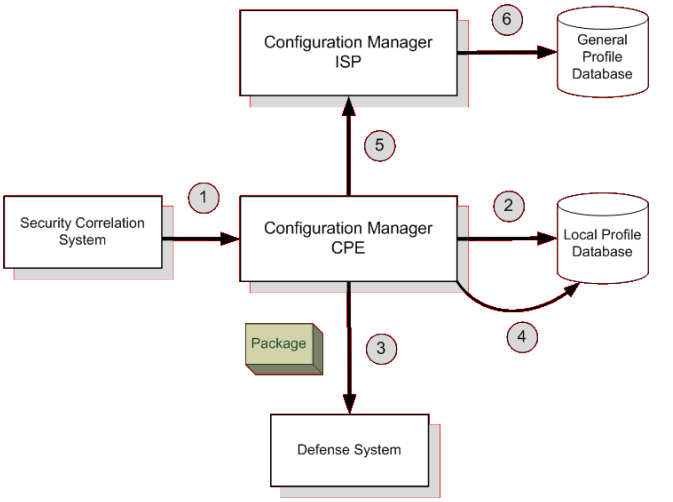

Fig. 6. Caso de uso de configuração dinâmica ao nível do operador de serviço.

C. *Entrada automatizada de dados no CPE*

O terceiro caso de uso (Fig. 7) corresponde à entrada de uma ordem de actualização dinâmica de parametrizações, emita pelo sistema de correlação de eventos do próprio CPE.

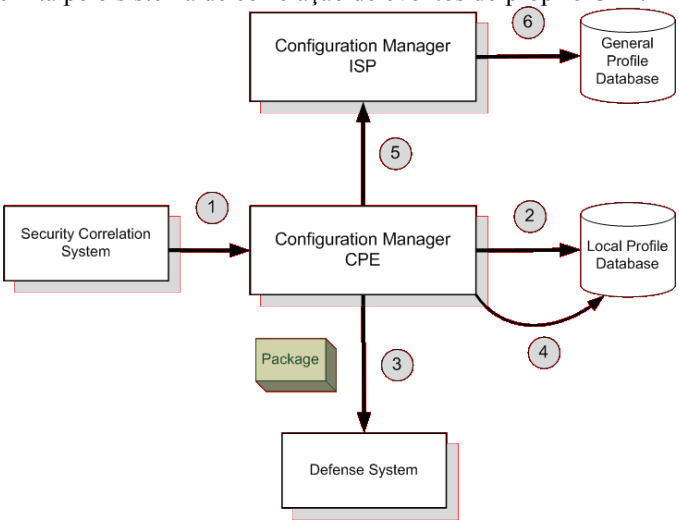

Fig. 7. Caso de uso de configuração dinâmica ao nível do CPE.

O motor de correlação de eventos de segurança do CPE decide, em resposta à detecção de actividade suspeita, alterar a parametrização de um serviço (por exemplo o *Iptables*). Emite então um comando nesse sentido para o *Configuration Manager* local (1). É realizado um procedimento análogo ao do caso de uso anterior, mas exclusivamente a nível local. Por último, todas as alterações que são realizadas na base local são replicadas na base de dados do operador de serviço (5), de modo a evitar inconsistências.

VI. Conclusão

A gestão de configurações de CPE, no contexto das redes de acesso de banda larga, assume hoje uma particular importância. Por um lado, é cada vez maior o número de dispositivos na rede doméstica do cliente relativamente aos quais o operador de serviço tem, de modo directo ou indirecto, responsabilidades de administração. Por outro lado, esses dispositivos asseguram serviços cada vez mais críticos (telefonia, televisão, *video-on-demand*, alarmes de intrusão, detectores de gás e inundações, televigilância, etc.) que os utilizadores pretendem que funcionem sem falhas.

Apesar do recente surgimento de normas para gestão remota de CPEs – em especial o TR-069 do *Broadband Forum*, que parece estar a ter gradual aceitação por parte dos fabricantes de equipamentos – continuam a não existir soluções adequadas e suficientemente flexíveis para gestão de configurações de CPE, limitando-se a maior parte das soluções actuais à distribuição de imagens monolíticas de todo o *firmware* do CPE, sem uma gestão dos binários serviço a serviço e sem qualquer gestão das parametrizações colocadas em cada CPE.

Embora existam já algumas das tecnologias necessárias, há ainda alguma dificuldade em fornecer um serviço de gestão de configurações suficientemente flexível para suportar múltiplos CPE, múltiplos perfis de serviço e múltiplos perfis de utilização. Adicionalmente, faltam também mecanismos adequados para suportar alterações dinâmicas de parametrização de componentes (e.g. *firewalls*).

Neste contexto, este artigo apresentou uma plataforma de gestão de configurações que tenta responder a estes desafios, sem deixar de se manter alinhada com as tecnologias preconizadas pelo *Broadband Forum*. Esta plataforma foi implementada e integrada na plataforma S3P, tendo também sido testada numa rede piloto.

Agradecimentos

O trabalho apresentado neste artigo foi parcialmente suportado pelo Programa Alβan, por meio da Bolsa de Mestrado com referência E07M403655BR.

Os autores gostariam de agradecer aos restantes membros da equipa do Projecto S3P pelo apoio, sugestões e comentários recebidos durante a execução deste trabalho.

Referências

[1] T. Cruz et al., “Segurança em redes de acesso Triple Play," Actas da 4ª Conferência Nacional sobre Segurança Informática nas Organizações (SINO 2008), Coimbra, Novembro de 2008.
[2] Home gateway initiative. http://www.homegatewayinitiative.org
[3] Broadband Forum. http://www.broadband-forum.org
[4] HGI, “Home gateway technical requirements: Residential profile version 1.0." 2008.
[5] G. Bathrick and H. Kirksey, “TR-069: CPE WAN management protocol," tech. rep., Broadband Forum, 2006.
[6] iPass. http://www.ipass.com, Julho 2009.
[7] Axiros. http://axiros.com
[8] Gatespace. http://www.gatespace.com
[9] Worksystems. http://www.workssys.com
[10] Dimark website. http://www.dimark.com
[11] B. Khosravifar and J. Bentahar, “An experience improving intrusion detection systems false alarm ratio by using honeypot,” in Advanced Information Networking and Applications, 2008. AINA 2008. 22nd International Conference on, pp. 997–1004, 2008.
[12] T. Cruz et al. “How to cooperatively improve broadband security,” Proceedings of the 8th European Conference on Information Warfare and Security (ECIW09), Lisboa, Julho de 2009.
[13] Netfilter Iptables. http://www.netfilter.org/pro jects/iptables/index.html
[14] Squidguard. http://www.squidguard.org
[15] Apt. http://wiki.debian.org/Apt