Relatório

Introdução

No âmbito da disciplina de Gestão e Segurança de Redes, foi executado um projeto cujo objetivo era a realização e montagem de uma rede representativa da realidade de uma pequena empresa. Este relatório procura explicitar o progresso, objetivos e dificuldades encontradas aquando da realização da segunda entrega do projeto.

Objetivos finalizados/Dificuldades encontradas

A segunda parte do projeto consistiu em aumentar a segurança da rede da ContaTudo, limitando o seu acesso aos elementos autorizados e recorrendo a serviços seguros.

Começámos criar uma nova máquina, ligada ao router do ISP, para uso do administrador que iria ter acesso de super-utilizador aos 5 servidores da ContaTudo. Atribuímos-lhe o endereço 10.0.0.34/30. O administrador acede aos servidores públicos por autenticação por chave pública e aos servidores privados pelos túneis SSH. Não fizemos scripts mas escrevemos no local.startup as configurações necessárias para realizar o túnel entre administrador e proxy (servidor público que escolhemos) e proxy e servidor de MRTG (servidor privado que escolhemos).

Quanto ao HTTPS redireccionámos automaticamente com sucesso o acesso ao site clientes.contatudo.gsr por HTTP para o mesmo site por HTTPS. Já o acesso ao site intranet.contatudo.gsr foi impedido para máquinas exteriores à rede ContaTudo.

Em relação ao DNS na primeira entrega já usávamos a relação master/slave entre servidores DNS primário e secundário mas agora reforçámos com a segurança na comunicação entre os dois através de uma chave secreta partilhada entre os dois servidores. Metemos ACL's para impedir e mudámos o allow-recursion para impedir que os servidores DNS da ContaTudo resolvessem pedidos DNS de zonas diferentes de contatudo.gsr para máquinas no exterior da rede da ContaTudo. Implementámos também o reverse DNS tanto na contatudo.gsr como na bomcliente.gsr.

Para a firewall, implementámos as suas regras no router_sede de forma a aceitar apenas as especificações do enunciado. Todas as máquinas com endereço IP público existentes no interior da rede da ContaTudo acedem à Internet sem restrições (excepto HTTP e início de ligação) e do exterior não se acede a nenhuma das máquinas com endereçamento privado. Também se acede aos servidores públicos apenas através do serviço que disponibilizam com função primária e nenhum utilizador do exterior consegue usar o proxy. De resto não é possível iniciar uma ligação do exterior para nenhum dos PCs da ContaTudo com IP público, embora seja possível iniciar uma ligação destes para o exterior, enquanto que os visitantes não têm quaisquer restrições de acesso à Internet em ambos os sentidos. Por fim, ataques de spoofing também foram prevenidos e impedidos com a criação de regras na firewall.

Usámos uma lógica negativa na firewall (damos ACCEPTS nas portas associadas aos protocolos que necessitamos, nas interfaces em causa, e no fim fechamos todas as portas restantes

dessas interfaces com um DROP geral). Usamos uns DROPS no meio dos ACCEPTS mas apenas porque são estritamente necessários naquela posição, para a lógica que utilizámos.

Depois implementámos um serviço VPN no servidor de DNS secundário para que pudesse trabalhar remotamente como se estivesse no interior da ContaTudo. Dentro da VPN só funcionam pings, traceroutes e digs. A VPN não dá acesso à Internet e foi necessária a criação de mais regras na firewall.

Finalmente, para a proxy Web foram implementadas mais regras na firewall e a flag "transparent" no porto 3128 do squid para impedir acessos HTTP sem ser do proxy e para enviar todos os pedidos HTTP dos visitantes para o proxy.

Nota: É possível aceder a um endereço privado dos administradores dos escritórios através dos visitantes pois não precisam de passar no router_sede, onde está a firewall, para comunicar um com outro. Esta medida de segurança não foi implementada pois não é requerida no enunciado.