Relatório do Projecto
GRS

Bernardo Simões 63503
Guilherme Vale 64029

1.Atribuição de Endereços

/*O ISP fornece à empresa o bloco 190.12.130.0/23, que esta divide de algum modo pelas suas sub-redes e
máquinas. Justifique as suas opções em relação a esta divisão.*/

Como a empresa tem três sub-redes, a divisão do bloco de IPs que o ISP fornece 190.12.130.0/23 foi feita da seguinte forma:
A sub-rede da empresa, que contem os Pcs dos vários pisos, atribuimos a gama de de Ips 190.12.130.0/24 (CIDR).Atribuimos uma grande gama de Ips de maneira a ser possivel aumentar o numero de pcs da empresa sem alterar a mascara de rede.

Na sub-rede da DMZ atribuimos a gama de ips 190.12.131.0/27 (CIDR). Atribuimos uma gama de ips menor do que na sub-rede anterior porque a DMZ da empresa só vai conter alguns servidores de serviços que teram de ser acedidos pelo exterior, logo será sempre uma sub-rede de menores dimenssões.

Na Sub-rede que liga o router da empresa ao router do isp usamos a gama de ips do ISP, 190.12.128.0/27

2.Firewall

Para fazer firewall usamos uma whitelist para indicar qual o trafego que pode aceder à sub-rede. Escolhemos usar whitelist em vez de blacklist, porque nas whitelist todo o trafego é bloqueado, apenas passa o trafego a que é dado permissões. Como as blacklist apenas indicam o trafego que tem permissões de entrar na rede, escolhemos a implementação por whitelist. Desta forma as firewalls bloqueiam todo o tráfego, deixando apenas passar o tráfego relacionado com os serviços (e-mail, Web, DNS e DHCP).

2.1 Firewall Router

Para que o servidor webmail seja acedido de dentro e fora da empresa, criamos uma premissão na firewall para que a DMZ possa receber pedidos e enviar respostas, HTTP (TCP porto 80), POP3(TCP porto 110), IMAP(TCP porto 143) , SMTP(TCP porto 25) e DNS (UDP porto 53) .
Para que o DHCP seja apenas acedido de dentro da empresa, colocamos uma premissão na firewall de maneira a permitir pedidos (UDP porto 68) e respostas (UDP porto 67) DHCP, de dentro da empresa.
Para permitir fazer ping ás máquinas demos premissões ao tráfego ICMP.
O tráfego externo a rede apenas consegue aceder á DMZ da empresa.

2.2 Firewall Bastião

De maneira a que a rede interna da empresa tenha apenas acesso aos serviços (e-mail, Web, DNS e DHCP) , a firewall do bastião bloqueia todo o trafego que não esteja relacionado com estes serviços. Para ser possível fazer ping, é permitido tráfego ICMP.

Escolhemos colocar os serviços de e-mail, Web e DNS, na DMZ (demiliterized zone) porque estes serviços têm de ser acedidos tanto de dentro como de fora da empresa.
Colocamos o serviço de DHCP dentro do router da empresa, porque este é o nó central da empresa. O serviço de DHCP apenas é acedido pela rede interna.