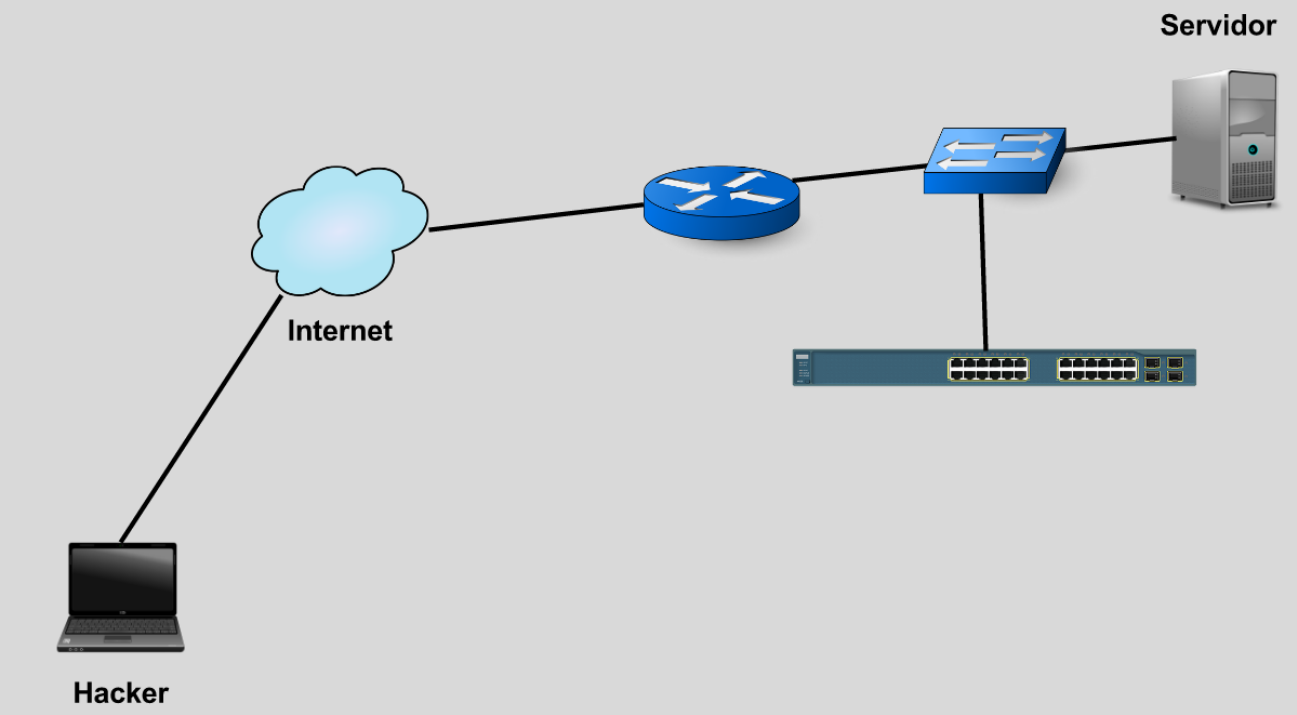
01

Conhecendo o firewall

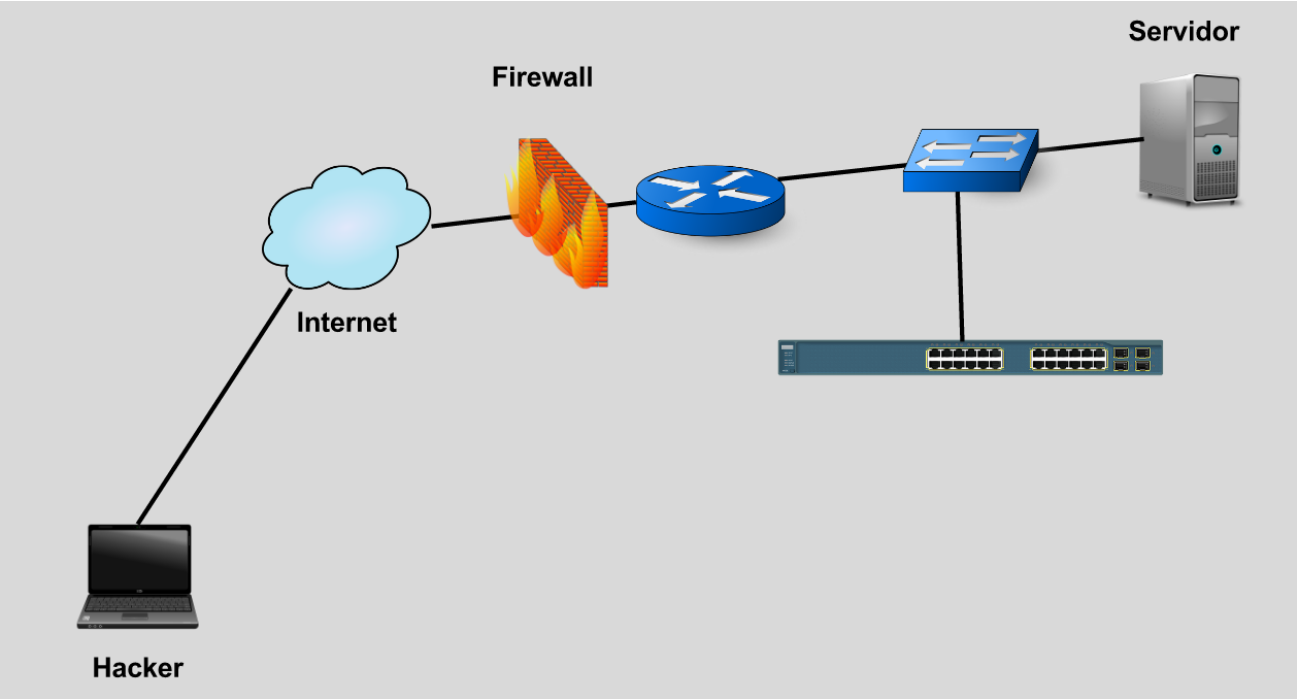
Transcrição

Já realizamos os ataques de DoS, realizamos varredura de portas com o Nmap e testamos as vulnerabilidades do servidor de maneira automatizada com o Nessus. Suponha que recebemos a notícia de que o presidente da empresa em que trabalhamos será alocado em nossa base.

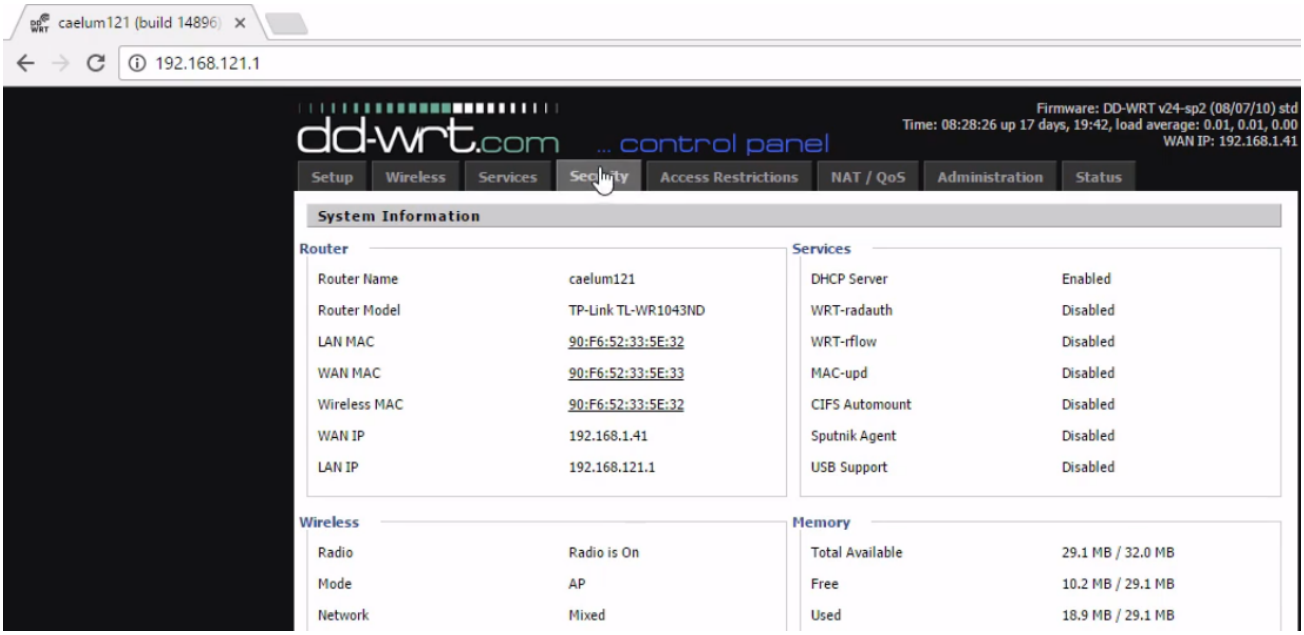


Podemos conectar o computador dele direto na porta do nosso switch, mas será que essa é a melhor das ideias? Temos um servidor web, que pode ser acessado por usuários da internet. Temos equipamentos como o IDS e o IPS, que ajudam a combater esses ataques, mas infelizmente nenhum equipamento de segurança é 100% infalível. Mesmo porque exploits são desenvolvidos por hackers de forma contínua, e novas vulnerabilidades são descobertas a cada dia.

Seria melhor se conseguíssemos separar a rede em regiões diferentes: uma que possa ser acessada por usuários da internet e uma que seja somente de uso interno. Para separar a rede nessas regiões de segurança distinta, pediremos ajuda para um equipamento chamado firewall.

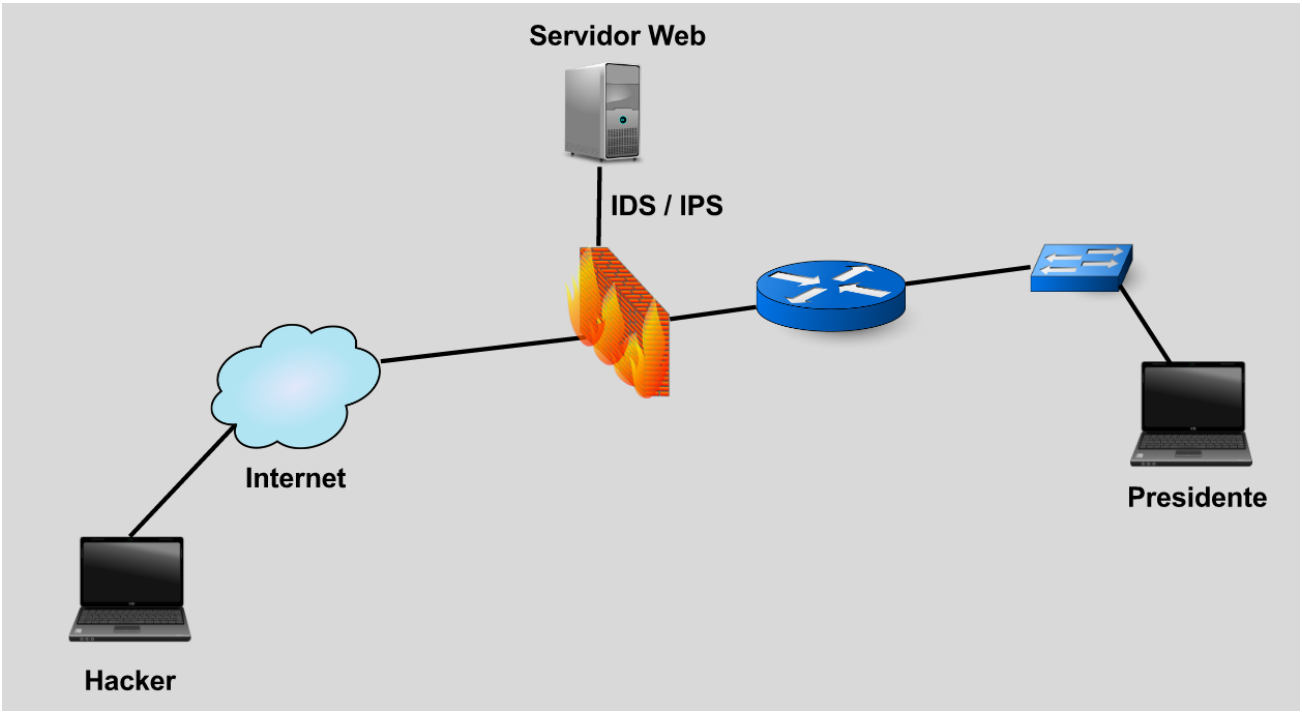


O firewall pode vir embutido no roteador ou pode ser um equipamento dedicado, normalmente encontrado em redes corporativas ou comerciais. Para ver as configurações do firewall do computador que estou usando, basta digitar o IP do roteador no navegador. Dentre as especificações, teremos uma aba de segurança (`Security`).

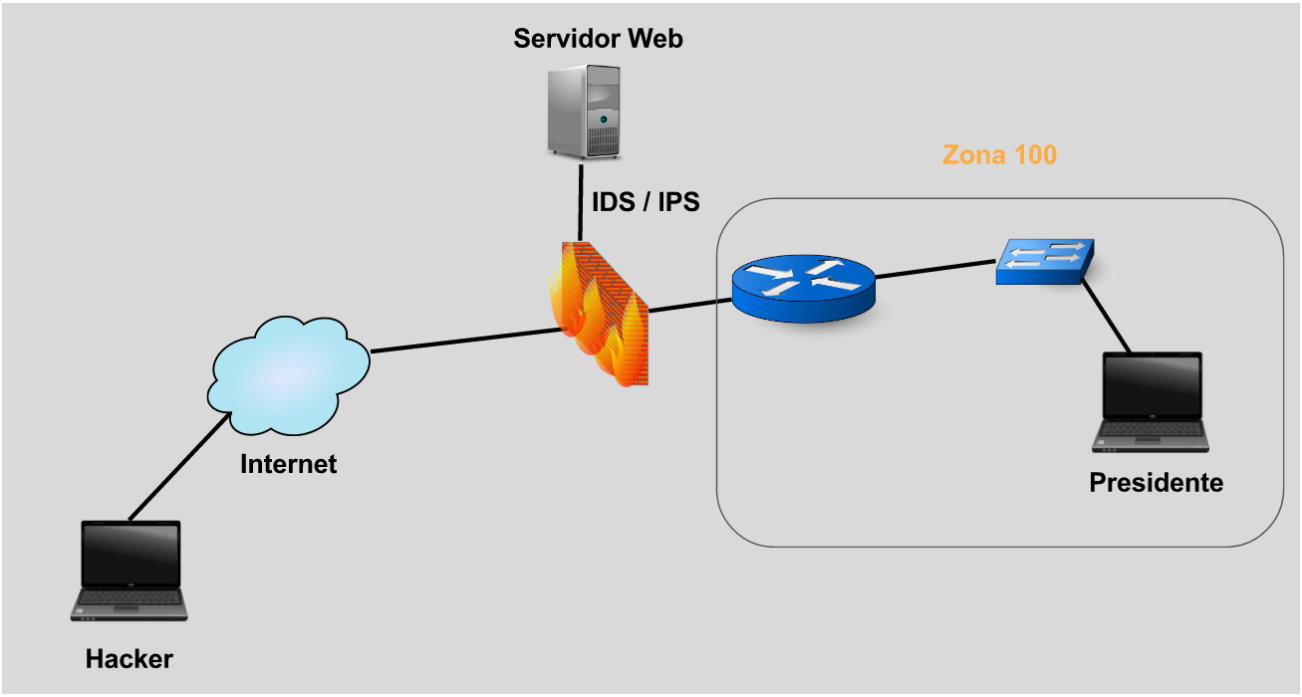


As configurações de um firewall doméstico são um pouco mais simples do que as de ambientes empresariais, que são o nosso foco. A aparência de um firewall empresarial é a seguinte:

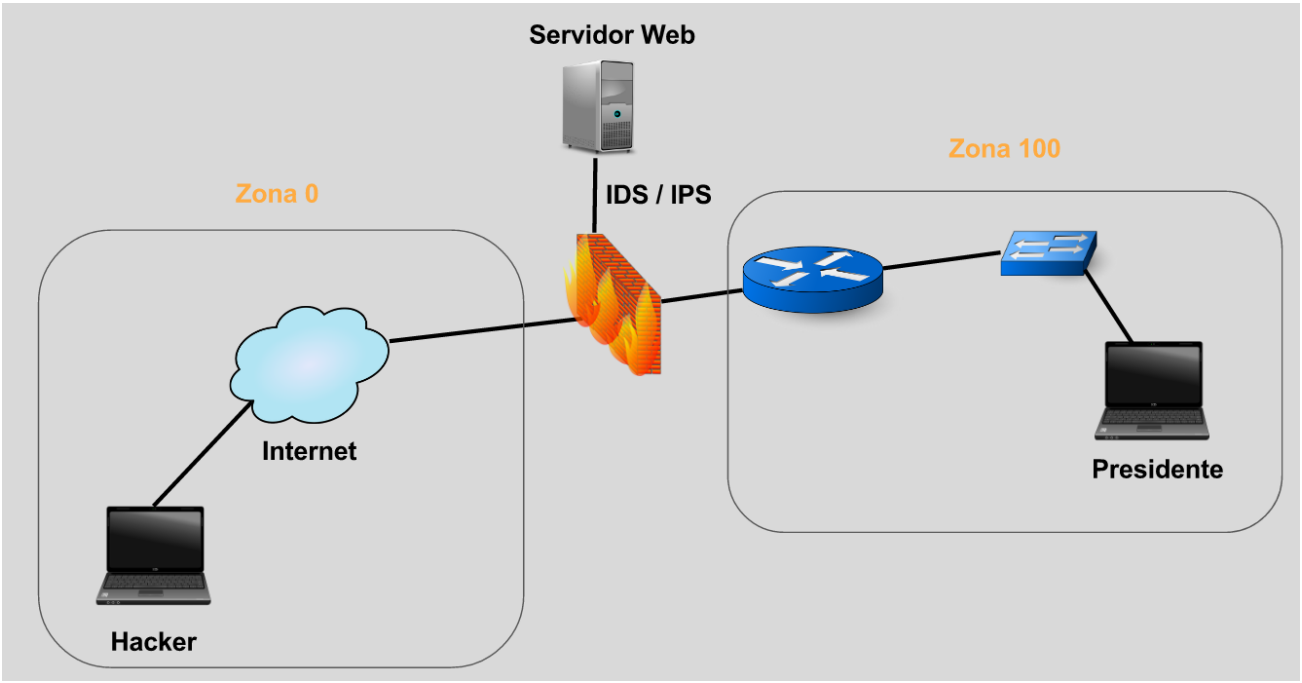
Ele possui as 4 interfaces que conseguimos ver na imagens, e é por elas que conseguimos fazer a divisão das redes em zonas de segurança.



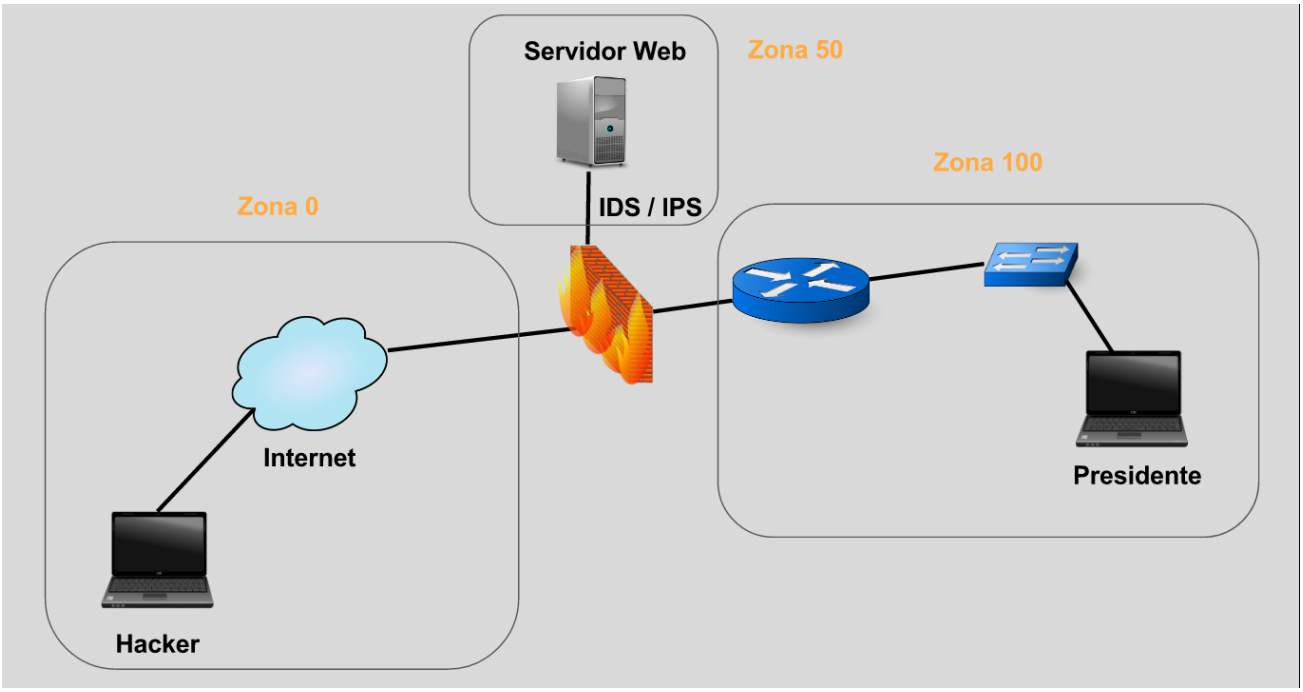
As redes que trabalham com um firewall selecionam o nível de segurança de cada parte da rede. Sabemos que a rede interna é segura, pois teoricamente temos controle sobre o que acontece sobre ela. Assim, comunicamos à interface do firewall à qual ela está conectada que essa rede é uma zona de alta segurança, por exemplo, zona 100.



Não sabemos o que pode vir da interface conectada à internet, que não está sob o nosso domínio. Pode haver usuários mal intencionados e hackers, então a classificaremos como zona 0.



Ainda temos o servidor web. Ele não está em uma zona totalmente segura, pois ele precisa ser acessado por usuários da internet. Mas não é tão insegura, pois é um equipamento da empresa e temos algum controle sobre o que acontece. Assim, sendo uma zona intermediária, a chamaremos de zona 50, também chamada de zona demilitarizada (DMZ).



Agora que as zonas de segurança estão divididas, qual será o funcionamento padrão dessa rede? De maneira parecida com a lei da gravidade, ou como uma cachoeira.

Suponha que a cachoeira tem 100 metros de altura, considerando a parte de baixo como 0. De acordo com a lei da gravidade e com o fluxo da água, o que está a 100 metros chega facilmente em 0. Mas o que está a 0 metros precisa da aplicação de uma força exterior para chegar à posição 100. O firewall funciona da mesma forma.

Imagine que o presidente da empresa, que está na zona 100, queira acessar o site da Alura. O servidor desse site está na internet, em uma zona de baixa segurança. O firewall vê que há informação sendo levada de uma zona segura para uma de baixa segurança, e como a zona 100 está acima da zona 0, a informação passa facilmente.

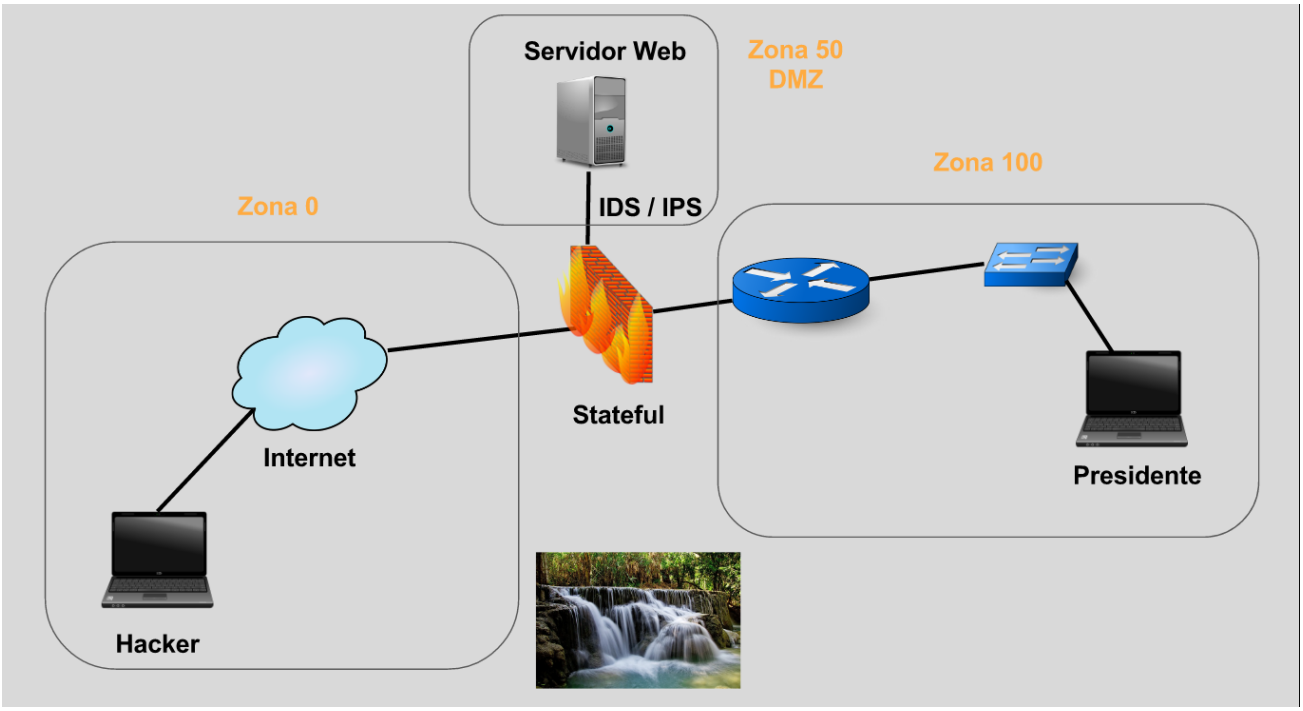
Quando o presidente precisa acessar o servidor web de sua empresa, a mesma coisa acontece: seu pacote de informações estará saindo de uma zona de alta segurança para uma DMZ. Seguindo a lei da gravidade, o pacote não terá dificuldades para chegar. Tudo isso por padrão.

Também por padrão, suponha que um hacker queira acessar algum recurso da rede interna. Depois de sua máquina gerar o pacote de informação, ele chegará ao firewall, que verá que foi gerado em uma zona não segura, a zona 0, e quer ir para a zona mais segura de todas. Como 0 é menor que 100, e isso vai contra a lei da gravidade, o firewall não permite que essa informação passe. Isso também acontece se um usuário da internet quiser acessar o servidor, pois 0 também é menor que 50. Para permitir que usuários da internet acessem o servidor, é preciso configurar uma exceção no firewall que permita que isso aconteça.

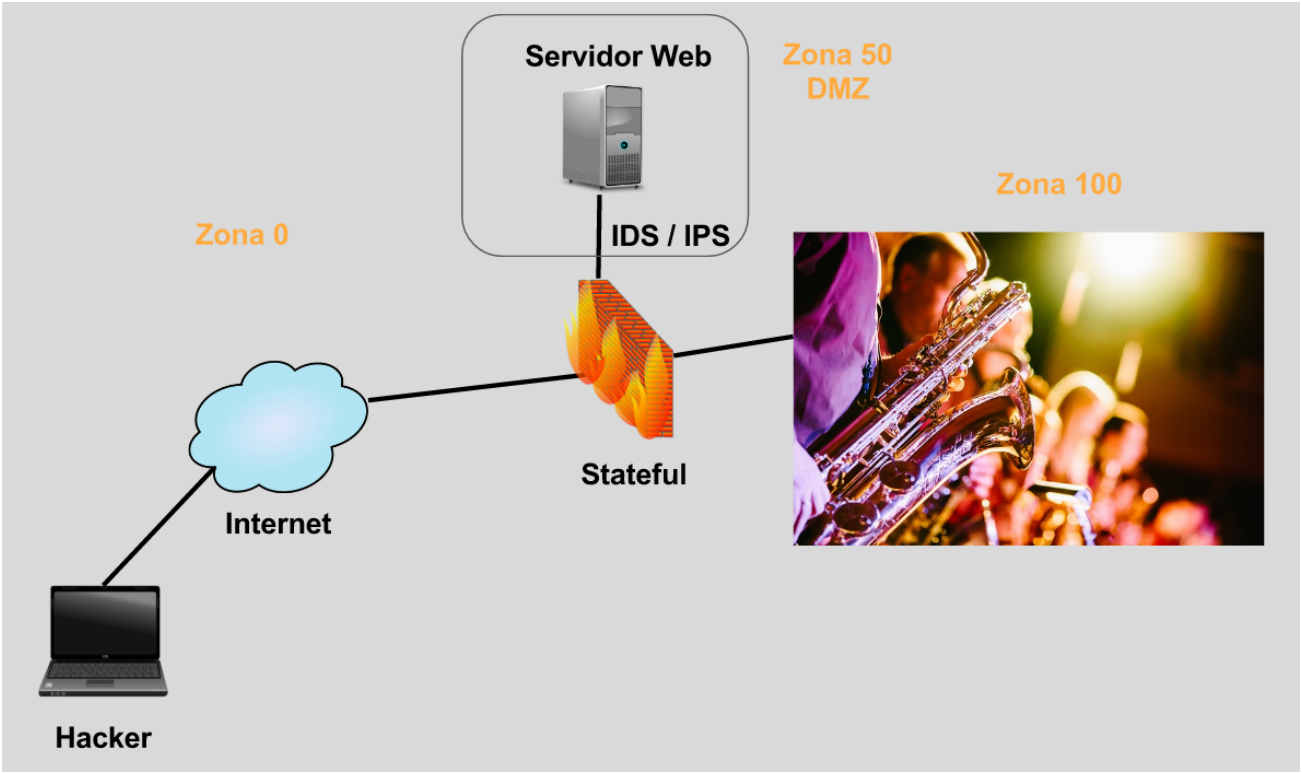
Ao separar a rede em regiões de segurança, conseguimos gerar uma maior segurança para a rede interna da empresa.

Mas sabemos que o presidente de nossa empresa quer acessar os cursos da Alura. Para isso, ele acessa o site e o servidor da Alura, que está em algum lugar da internet, devolve um pacote de informações que deve voltar para a rede interna. Só assim o site aparecerá na máquina do presidente.

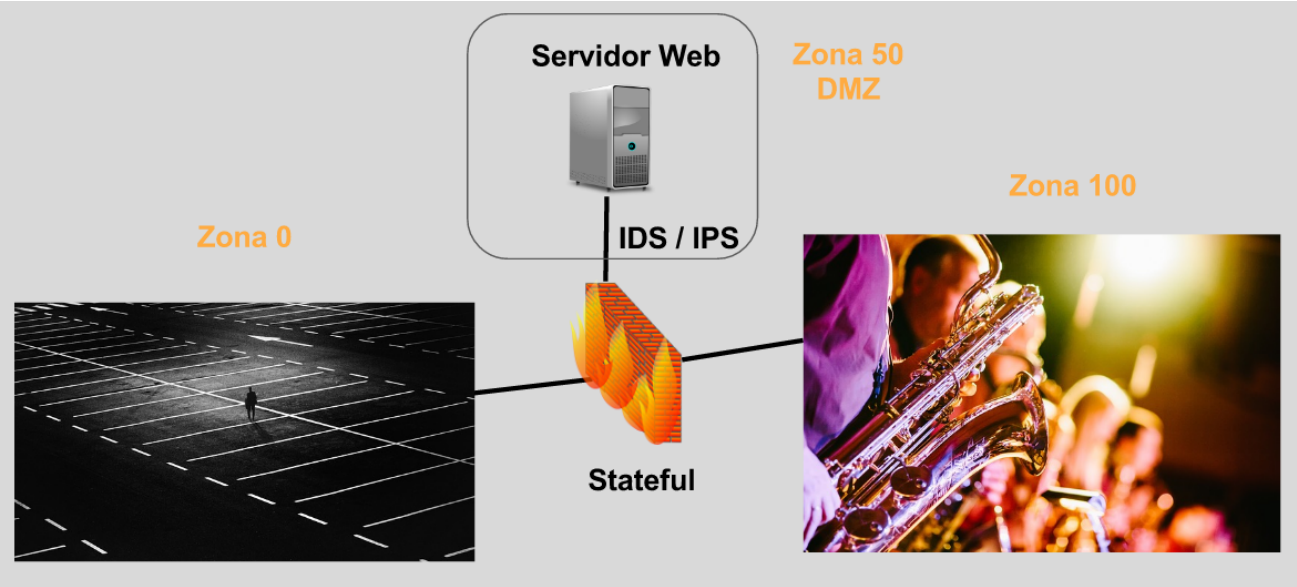
Mas como acontecerá esse retorno? A informação deve ir da zona 0 para a zona 100. Será que devemos configurar uma exceção para que sites consigam acessar a rede interna? Não faria sentido, senão o firewall não teria grande utilidade. Felizmente, os firewalls possuem uma memória chamada *stateful*.



Para entender como essa memória funciona, vamos mudar a analogia. Suponha que a rede interna seja uma casa de shows.



Nosso celular toca, e é um amigo que está do lado de fora dessa casa. Ele está um pouco perdido, e pergunta se podemos sair para encontrá-lo do lado de fora e depois entrarem juntos.



Passaremos pelo portão de entrada, o firewall, que tem um segurança. Explicamos a situação para ele, e avisamos que queremos passar para buscar o nosso amigo e voltar em breve. Como o segurança é um cara legal, ele vai nos dar permissão para fazer isso.

Então, vamos buscar nosso amigo. Na volta, é preciso passar pelo portão de entrada novamente, e perguntar para o segurança se ele vai nos deixar entrar novamente. O segurança se lembrará de você e permitirá que entre novamente.

O firewall funcionará de maneira similar. Quando o presidente digita a URL da Alura em seu computador, esse pedido vai passar pelo firewall, que o salvará em sua memória stateful, junto com seu IP e suas portas de comunicação. Quando essa informação sair e chegar ao servidor da Alura, ele verá essa requisição de acessar o site e devolverá informação. Quando essa informação chegar na porta do firewall, será comparada à tabela de memórias. Ele verá que esse tráfego é uma resposta a uma ação anterior, vinda da parte segura da rede. Essa comparação envolve portas e número de IP. Ao ver que essa informação é um retorno que vem da rede interna, graças à sua memória, ele vai permitir que esse tráfego entre na parte segura. E então o presidente poderá acessar o site da Alura.

O firewall não aceitará, por padrão, que um tráfego originado da internet entre na rede interna. Ele permitirá que ele entre apenas se alguém de dentro faça uma requisição, e o pacote de informações seja um retorno à essa requisição. Pensando nisso, como o hacker por tentar acessar e comprometer o computador de uma vítima que esteja na rede interna?

Vamos pensar juntos no que o hacker teria de vantajoso do lado dele. Se, de alguma forma, o computador do presidente iniciasse uma conexão com o computador do hacker, no retorno o firewall poderia pensar que esse pacote seria a resposta de uma requisição gerada pelo presidente. Assim, o hacker poderá ter acesso ao computador do presidente, pois a requisição teria sido feita por ele.

Hoje em dia os firewalls possuem uma proteção grande contra essas políticas e protocolos. Eles geralmente conseguem verificar se um protocolo está sendo usado de forma indevida, mas depende muito do fabricante. Por isso, é uma das possibilidades que o hacker tem.

Portanto, ele tentará mandar um vírus para o presidente, para que ele clique nesse arquivo e inicie uma conexão com o computador do hacker. E, pelo fato de ser um computador da rede interna iniciando essa conexão, o firewall poderá aceitar esse retorno. Assim, o hacker passará a segurança e poderá ganhar controle da máquina do presidente.

Como a conexão se inicia no sentido contrário ao ataque, que vem do hacker, é chamada de conexão reversa, em inglês *Reverse Shell*. Tentaremos, na próxima etapa, criar esse arquivo, que dependerá muito do sistema operacional e outros

fatores. Veremos juntos o que pode acontecer nesse tipo de ataque, a partir de quando recebemos o vírus, e quais são as vulnerabilidades expostas. Até lá!