UNIVERSIDADE DE AVEIRO



Departamento de Eletrónica, Telecomunicações e Informática

Segurança em Redes de Comunicações

Relatório do Projeto 1

Load-Balancing Scenario (with redundancy and state synchronization)

Uma imagem com diagrama, texto, file, mapa

Descrição gerada automaticamente

Adalberto Júnior Vaz do Rosário

105589

19/04/2024

**Explain why the synchronization of the load-balancers allows the nonexistence of firewall synchronization.**

Neste cenário, como todo o tráfego tem de passar por load-balancers, antes de chegar às firewalles, e como tanto os que têm acesso à rede interna quanto os que está conectado à rede de fora, são sincronizados via VRRP, isso permite uma “sincronização implícita” entre firewalles. Isso significa que no caso de tradução de endereços (NAT/PAT) os load-balancers direcionam o tráfego para o firewall correspondente que traduziu o IP, superando assim a necessidade dos firewalles sincronizarem suas tabelas de tradução NAT/PAT.

**Which load balancing algorithm may also allow the nonexistence of load-balancers synchronization?**

**IP Hash**

No algoritmo IP Hash, o load-balancers combina os endereços IP de origem e destino do tráfico de entrada e usando uma função matemática converte essa combinação em um hash. Este hash é usado para atribuir a conexão a um servidor específico, isso significa que todas as requisições de um mesmo cliente sempre serão direcionadas de forma consistente para o mesmo servidor e os tráficos será balanceada uniformemente desde que haja uma consistência de função hashing em todos os servidores. E isso permite a não necessidade de sincronização.

**Explain why device/connection states synchronization may be detrimental during a DDoS attack.**

Os ataques DDoS sobrecarregam os sistemas com um fluxo massivo de conexão. A sincronização dos estados do dispositivo/conexão adiciona outra camada de processamento para sistemas já sobrecarregados. Isso pode consumir recursos valiosos necessários para lidar com conexões legitimas ou identificar e mitigar o próprio ataque. E alem disso pode haver potencial inconsistência na rede, isto porque pode haver dificuldade por parte dos protocolos de sincronização para acompanhar as rápidas mudanças, levando a desatualização dos dados ou informações imprecisas sobre os estados dos dispositivos.

**Topologia**

Uma imagem com diagrama, texto, file, mapa

Descrição gerada automaticamente

Uma imagem com texto, Tipo de letra, branco, design

Descrição gerada automaticamenteUma imagem com texto, Tipo de letra, branco, captura de ecrã

Descrição gerada automaticamente

A rede é composta por três zonas: INSIDE, OUTSIDE e DMZ. Na zona INSIDE (rede interna), existem 3 sub-redes. A rede 10.2.2.0/24, que chamei de Rede Marketing, que contem um VPCS com o endereço IP 10.2.2.100, a rede 10.3.3.0/24, que chamei de Rede Admin, contém um VPCS com IP 10.3.3.5 e a rede 10.4.4.0/24, chamado de Rede de Servidor de Dados, contém um VPCS com o endereço IP 10.4.4.100. Os restantes IPs da rede 10.0.0.0/8 são designados para os restantes terminais da empresa.

A zona OUTSIDE(Internet) consiste na sub-rede 200.2.2.0/24 com um VPCS para simular um dispositivo externo.

Por ultimo, a zona DMZ inclui a sub-rede 192.1.1.0/24 com três endereços IP, sendo: 192.1.1.100 que é o IP do (DMZ)Server sendo apena acessível internamente, 192.1.1.150 servidor da pagina publica da empresa e o 192.1.1.200 que simulará um servidor DNS.

**CONFIGURAÇÕES (Os pontos relevantes)**

**INSIDE e OUTSIDE**

No router Inside (R1) defini rotas estáticas para LB1A e LB1B, enquanto no router Outside (R2) configurei rotas estáticas para LB2A e LB2B.

**Load Balancers (LBs)**

Todos os LBs, com exeção ao LBDMZ possuem conntrack-sync configurado na eth5, e balanceamento de carga em suas interfaces eth1 e eth2 com pesos iguais, isso significa que a probabilidade de encaminhar um pacote para uma interface é de 50%. Nos LB1 criei rotas estáticas encaminhando as redes dos departamentos internos para a interface do router Inside e nos LB2 há rota estática direcionando o tráfico para a rede 200.2.2.0/24 pelo router Outside.

**FIREWALLs (FW)**

Para os Firewalls (FWs), configurei rotas estáticas de INSIDE para OUTSIDE e de OUTSIDE para INSIDE. O tráfego destinado à rede 10.0.0.0/8 é direcionado através dos próximos saltos conectados às interfaces eth1 e eth2, enquanto o tráfego destinado à rede 200.2.2.0/24 é roteado através dos próximos saltos ligados às interfaces eth0 e eth3. Também ativei o serviço SSH na porta 22, dando controle de acesso ao utilizador padrão (vyos) e apenas dispositivos conectados a interface eth4 podem acessá-lo através de SSH. **(Para parte Extra)**

O pool NAT entre FWs são iguais, usando um pool que varia de 192.168.1.0 a 192.168.1.10.

**Uma imagem com texto, captura de ecrã, software, Software de multimédia

Descrição gerada automaticamente**

**Políticas (Serviços)**

Definir alguns serviços para redes. A rede Inside só pode comunicar com a rede Outside utilizando UDP nas portas 6000 a 7000. O Outside não pode iniciar uma comunicação com o Inside.

Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente

Outro serviço foi o acesso do Inside à DMZ. Todos os dispositivos internos podem executar ping em dispositivos na rede DMZ, comunicar-se por UDP na porta 53 (para simular uma comunicação DNS) e também comunicar-se via TCP nas portas 80 e 443, permitindo-lhes acessar serviços web por HTTP e HTTPS. Além disso, apenas a rede administrativa (10.3.3.0/24), por enquanto somente o IP 10.3.3.5/32 pode se comunicar com a DMZ através de TCP na porta 22, o que significa que somente os administradores podem estabelecer conexões SSH com os terminais dentro da DMZ.

Somente a rede do Data Server(10.4.4.0/24) pode se comunicar com a DMZ através de TCP na porta 21,57 e 587 para simular os serviços FTP, MTP e SMTP respetivamente e através de UDP na porta 18 para simular SMP(Message Send Protocol).

Uma imagem com texto, captura de ecrã, menu, Tipo de letra

Descrição gerada automaticamente Uma imagem com texto, captura de ecrã, menu

Descrição gerada automaticamente Uma imagem com texto, captura de ecrã

Descrição gerada automaticamente Uma imagem com texto, captura de ecrã, menu, Tipo de letra

Descrição gerada automaticamente Uma imagem com texto, Tipo de letra, captura de ecrã

Descrição gerada automaticamente Uma imagem com texto, Tipo de letra, captura de ecrã

Descrição gerada automaticamente

Notei que alguns portos não funcionam em todos VPCS mesmo tendo permissão e maioriam ping nessas portas só funcionam quando é feito para o PC da maquina virtual(192.1.1.100).

Talvez seja problemas de formatação de pacotes.

Uma imagem com texto, captura de ecrã, Tipo de letra, documento

Descrição gerada automaticamente

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

Para a rede OUTSIDE, defini um serviço no qual os dispositivos só podem se comunicar com o endereço IP 192.1.1.150 (página pública). Os métodos de comunicação permitidos são através de pings ou via TCP na porta 443, que permite acesso via HTTPS.

Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

A comunicação via TCP na porta 443 deveria funcionar mais por algum motivo não funciona. Não consegui compreender a causa da não funcionamento.

Funcionamento Correto: Só é permitido para o IP 192.1.1.150

Uma imagem com texto, captura de ecrã, Tipo de letra, design

Descrição gerada automaticamente Uma imagem com texto, captura de ecrã, Tipo de letra

Descrição gerada automaticamente

**A DMZ não tem permissão para iniciar uma comunicação, nem para Inside nem para o Outside.**

**Conclusão:**

**No decorrer do projeto deparei com alguns problemas que até então não consegui resolver. Por algum motivo após fechar o gns3 os vyos ficam inacessíveis no virtualbox, e não consigo voltar a abrir o projeto. Só consigo abrir o projeto se voltar a criar novamente as máquinas com os meus nomes do projeto e consequentemente perco os dados. Por algum motivo serviços implementados via portas não funcionam e os que funcionam são os feitos para uma máquina virtual e não para VPCS.**

**Para fazer o projeto usei como base relatório do grupo (**André Clérigo (98485), Pedro Rocha (98256)) **alunos do ano anterior. Usei algumas configurações usadas por eles, acrescentei algumas e também atualizei algumas que não faziam sentidos para a minha rede.**

**Links Usados:**

[mect\_1ano/SRC/Prática/projeto1/SRC\_\_Report\_1.pdf at main · andreclerigo/mect\_1ano (github.com)](https://github.com/andreclerigo/mect_1ano/blob/main/SRC/Pr%C3%A1tica/projeto1/SRC__Report_1.pdf)

[Protocolos de rede| Portas de rede | Cloudflare](https://www.cloudflare.com/pt-br/learning/network-layer/what-is-a-computer-port/)

[Lista de portas dos protocolos TCP e UDP – Wikipédia, a enciclopédia livre (wikipedia.org)](https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP)

[Service Name and Transport Protocol Port Number Registry (iana.org)](https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml)

[SRC - Access and Flow Control (ua.pt)](https://elearning.ua.pt/pluginfile.php/3322182/mod_resource/content/20/Flow_Control.pdf)