Impacto do Firewall, implementado via software, em uplink igual ou superior a 1Gbps

Cinfotec UNICAMP

16 e 17 de abril de 2013

Autor: Valcir Cabral Vargas – Instituto de Biologia

Introdução:

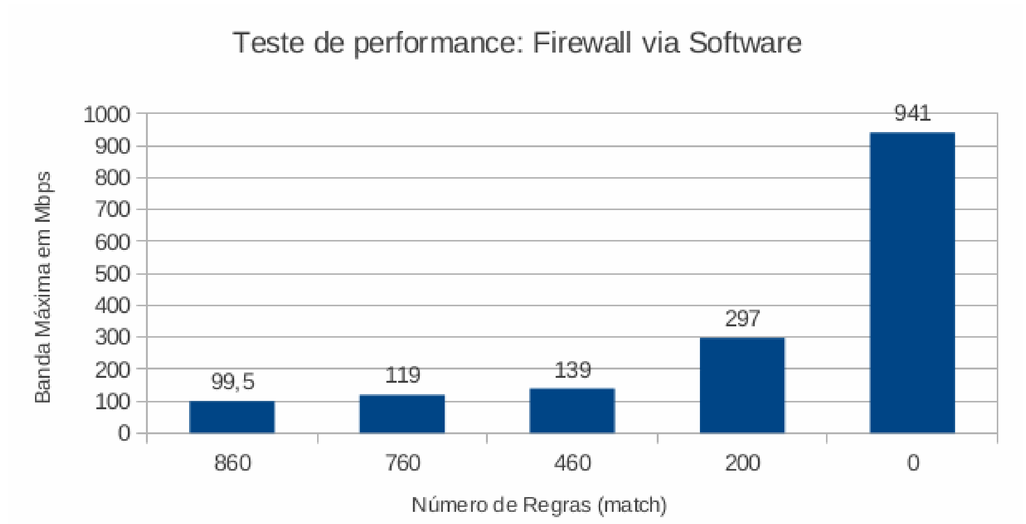
Firewall é um serviço que auxilia na segurança da rede. Sua responsabilidade é filtrar pacotes por endereço, porta ou protocolo. Firewall implementado via software é quando a função de filtragem é realizada por um servidor, exemplos: FreeBSD (IPFW) ou Linux (IPTABLES). Esta arquitetura, firewall via software, é amplamente adotada pelos administradores de rede da Unicamp. No Instituto de Biologia é utilizado a solução FreeBSD + IPFW, a mesma testada neste trabalho.

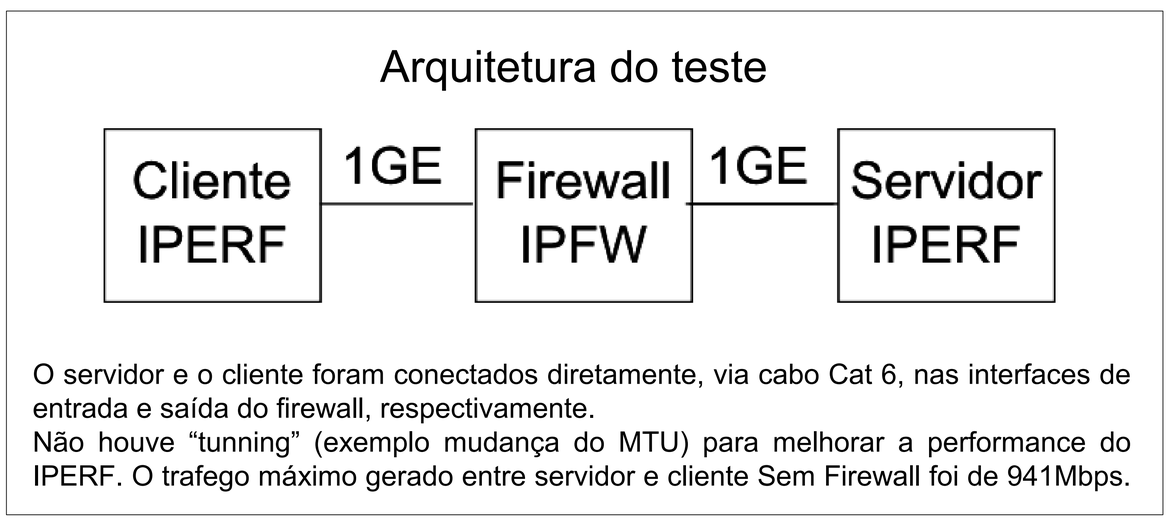
Objetivo:

Analisar o impacto que o firewall causa no limite de banda em uplink de 1Gbps ou superior e propor melhorias.

Resultado:

Testes de performance realizados com o iperf, um software livre para teste de banda, mostram o desempenho da rede em função do número de regras (filtros) do firewall. Um servidor Dell Power Edge 1950, 2 processadores + 4GB de RAM, foi utilizado na função de Firewall. E, mais 2 servidores (Supermicro 2 processadores quad-core com 16 GB de RAM), com iperf instalados na função de geradores de trafego. A quantidade de regras (filtros) impactam drasticamente no limite de banda, como mostrado no gráfico abaixo:





O servidor e o cliente foram conectados diretamente, via cabo Cat 6, nas interfaces de entrada e saída do firewall, respectivamente.
Não houve "tunning" (exemplo mudança do MTU) para melhorar a performance do IPERF. O trafego máximo gerado entre servidor e cliente Sem Firewall foi de 941Mbps.

A quantidade de regras igual a 0 (zero) indica que o Firewall foi desabilitado e apenas a função de encaminhamento de pacotes (ip_forward) estava ativada, neste caso não houve impacto na banda. No caso do teste com 460 regras, a banda foi reduzida para aproximadamente 15% (139Mbps) do montante (941Mbps).
O teste foi realizado com apenas um tipo de trafego para que o match (regra que "bate") fosse gerado. No entanto, em condições normais, o tipo de trafego é bem variado (FTP, HTTP, DNS,etc). Contudo, podemos observar abaixo que o pico de banda consumida pelas grandes unidades é muito abaixo dos 1Gbps:

Unidade	Banda Máxima em Mbps	Unidade	Banda Máxima em Mbps	Unidade	Banda Máxima em Mbps
IA	165	IFGW	195	CCUEC	296
IB	231	IQ	128	FEM	133
IC	175	DGA	166	CAISM	116
IG	82	CENAPAD	98	* FEEC	848

Informações retiradas do sistema de monitoramento do CCUEC:
http://www.ccuec.unicamp.br/monitor/mrtg2html/unicamp/nos.html
Data: 03/04/2013 (Obs: Apenas o *Maximal Incoming* foi considerado)

* A FEEC é a única unidade da relação que NÃO utiliza Firewall via Software.

Conclusão:

É notório o grande impacto causado pelo firewall implementado via software em uplink de 1Gbps ou superior. O fato também inviabiliza conexões sensíveis, como por exemplo TelefoniaIP e Vídeo Conferencia. Dá para melhorar a performance reduzindo a quantidade ou a ordem das regras, no entanto a melhoria é sutil e a segurança da rede pode ser comprometida, devido técnicas de sumarização, por exemplo.
A solução ideal para se atingir limite, próximo ou superior, a 1Gbps é a implementação de **Firewall via Hardware**. Contudo, esta nova arquitetura exigirá novos conhecimentos (principalmente em ACL) por parte dos Administradores de Rede da Unicamp e, em alguns casos, investimento em equipamentos (roteadores).
Roteador, também chamado de CORE, com implementação de ACL inbound e outbound em hardware é a melhor opção para interessados em alto desempenho.