WIPFW

Navegação:

- **Início**
- **Documentação**
- **FAQ**
- **Página do projeto**
- **Download**
- **Fóruns**
- **Contactos**

WIPFW documentação (v0.2.8)

Sinopse

```
ipfw [-q] adicionar [número] regra corpo
[AdeftN] {ipfw list | mostrar} [número ...]
ipfw [-f |-q] flush
ipfw [-q] {zero | resetlog | delete} [número ...]
```

```
ipfw [-Nq] pathname
```

Descrição

Uma configuração ipfw, ou conjunto de regras, é feito de uma lista de regras numeradas de 1 a 65535. Os pacotes são passados para ipfw em vários locais diferentes na pilha de protocolos (dependendo da origem e de destino do pacote, é possível que o ipfw é chamado várias vezes no mesmo pacote). O pacote passou para o firewall é comparado com cada uma das regras nas regras de firewall. Quando uma correspondência for encontrada, a ação correspondente à regra correspondente é executada.

Um conjunto de regras ipfw sempre inclui uma regra padrão (numerada 65535) que não pode ser modificado ou excluído, e corresponde a todos os pacotes. A ação associada com a regra padrão pode ser negar ou permitir que dependendo de como o kernel está configurado.

Se o conjunto de regras inclui uma ou mais regras com o manter o estado ou opção de limite, então ipfw assume um comportamento de estado, ou seja, sobre um jogo que vai criar regras dinâmicas que corresponda aos parâmetros exatos (endereços e portas) do pacote correspondente.

Estas regras dinâmicas, que têm uma vida limitada, são verificados na primeira ocorrência de um cheque do Estado, manter o estado-limite ou regra, e são typypically usado para abrir o firewall on-demand para o tráfego legítimo somente. Consulte o firewall dinâmico e Seções exemplos abaixo para obter

mais informações sobre o comportamento de stateful ipfw.

Todas as regras têm um associado contadores alguns: pacote, a contagem de um byte e contar um timestamp indicando o tempo do passado. Correspondem a uma contadores podem ser exibidas ou redefinir comandos com ipfw.

As regras podem ser adicionados com o comando add; individualmente apagados com o comando delete, ea nível mundial com o comando flush; exibido, opcionalmente, com o conteúdo dos contadores, usando o programa e os comandos da lista. Finalmente, os contadores podem ser repostas com o zero e resetlog comandos.

As opções disponíveis são as seguintes:

-Um	Enquanto a lista, mostrar os valores do contador. O comando show apenas implica essa opção.
-D	Embora anúncio, mostram regras dinâmicas, além de estáticas.
-E	Embora anúncio, se a opção-d foi especificado, também mostram expirou regras dinâmicas.
-F	Não pede confirmação para comandos que podem causar problemas se mal utilizada, ou seja, flush. Se não houver nenhum tty associada com o processo, isto é implícito.
-Q	Ao adicionar, zeragem, resetlogging ou rubor, ficar quieto sobre ações (implica-f). Isso é útil para ajustar as regras de execução de comandos ipfw múltiplas em um script (por exemplo, `rc.firewall sh"), ou pelo processamento de um arquivo de regras ipfw muitos, através de uma sessão de login remoto. Se uma descarga é realizada no modo verbose () normal (com a configuração padrão do driver), ele imprime uma mensagem. Como todas as regras são liberadas, a mensagem não pôde ser entregue para a sessão de login, fazendo com que a sessão de login remoto para ser fechado, eo restante do conjunto de regras não é processado. O acesso ao console seria então obrigada a recuperar.
T	Embora anúncio, mostram timestamp última partida.
-N	Tente resolver os endereços e nomes de serviço na produção.
enum	Mostrar lista de interfaces (somente para Windows).
sysctl	Mostrar valores sysctl. Você pode mudá-lo - por exemplo: "debug sysctl ipfw = 0"

Para facilitar a configuração, as regras podem ser colocadas em um arquivo que é processado usando ipfw, como mostrado na linha sinopse primeiro. Um caminho absoluto deve ser usado. O arquivo será lido linha por linha e aplicada como argumentos para o utilitário ipfw.

formato de artigo

O formato das regras ipfw é o seguinte:

> [Prob match_probability] acção [log [número logamount]] proto de src para dst [interface-spec] [options]

onde o corpo da regra especifica que a informação é usada para filtrar pacotes,

entre os seguintes:

Protocolo IPv4	TCP, UDP, ICMP, etc
Origem e destino do endereço IP	possivelmente mascarado
Fonte e porta de destino	listas, intervalos ou máscaras
Direção	(Entrada ou saída)
Transmitir e receber interface	Por nome ou endereço
Misc. campo de cabeçalho IP	Versão, o tipo de serviço, o comprimento do datagrama, a identificação, a bandeira fragmento (IP diferente de zero offset), Time To Live
Misc. campo de cabeçalho TCP	flags TCP (SYN, FIN, ACK, RST, etc), número de seqüência, número edgment-reco, janela
opções TCP	
tipos de ICMP	para pacotes ICMP

Note-se que algumas das informações acima, por exemplo, endereços IP e / UDP portas TCP, pode ser facilmente falsificado, para filtragem desses campos por si só pode não garantir os resultados desejados.

rule_number

Cada regra está associada a um rule_number na faixa de 1 .. 65.535, sendo o último reservado para a regra padrão. As regras são verificadas sequencialmente pelo número da regra. Várias regras podem ter o mesmo número, caso em que são verificados (e constantes) de acordo com a ordem em que foram adicionados. Se uma regra está inscrita sem especificar um número, o kernel irá atribuir um, de tal forma que a regra se torna a última antes da regra padrão. Números regra automática são atribuídos por incrementar o número da regra-padrão não passado em 100. Se isso não for possível (por exemplo, porque iríamos além da regra número máximo permitido), o mesmo número de valor não-padrão será usado o último lugar.

match_probability prob

Um jogo só é declarado com a probabilidade especificada (número de ponto flutuante entre 0 e 1). Isso pode ser útil para uma série de aplicações, tais como queda de pacotes aleatórios para simular o efeito de vários caminhos levando a fora-de-ordem de entrega de pacotes.

log [número logamount]

Quando um pacote corresponde a uma regra com a palavra-chave de registro, uma mensagem será registrada no windows \ security \ logs \ wipfwYYYYMMDD.log.
Quando o limite for atingido, o registro pode ser reativado por limpar o registro do contador ou o pacote contra a essa entrada, consulte o comando resetlog.
Nota:
registro será feito após todos os outros pacotes combinando condições foram verificados com sucesso e, antes de executar a ação final (aceitar, negar, etc) sobre o pacote.

ações da regra

Uma regra pode ser associada a uma das seguintes ações, que será executada quando o pacote de jogos do corpo da regra.

allow | aceita | passar | licença

Permitir pacotes que corresponde à regra. A busca termina.

estado de check-

Verifica o pacote contra as regras dinâmicas. Se for encontrada uma correspondência, executa a ação associada com a regra que gerou esta regra dinâmica, caso contrário, passar para a próxima regra.-Verificar as normas estaduais não têm um corpo. Se nenhuma regra do estado de seleção é encontrada, o conjunto de regras dinâmica é verificada no primeiro manter o estado-limite ou regra.

contagem

contadores de Atualização para todos os pacotes que correspondem a regra. A busca continua com a próxima regra.

negar | queda

Descarta os pacotes que correspondem a essa regra. A busca termina.

Número skipto

Passar todas as regras subsequentes numerados de um número menor. A busca continua com a primeira regra número numeradas ou superior.

corpo da regra

O corpo de uma regra contém zero ou mais padrões (como fonte específica e endereços de destino ou os portos, as opções de protocolo, ou enviadas interfaces de entrada, etc) que o pacote deve corresponder, a fim de ser reconhecido. O corpo de uma regra deve, em geral, incluir uma fonte de especificador e endereço de destino. A palavra-chave qualquer pode ser usado em vários lugares para especificar que o conteúdo de um campo de preenchimento obrigatório, é irrelevante.

O corpo da regra tem o seguinte formato:

> [Proto de src para dest] [options]

Regra campos têm o seguinte significado:

proto: Protocolo

Um protocolo IP a partir do modelo de referência TCP / especificado por número ou nome (para uma lista completa, veja windows \ system32 \ drivers \ protocol \ etc).
O IP ou todas as palavras qualquer protocolo irá corresponder.

src e dst: [portos] endereço IP

Um único endereço IP, opcionalmente seguido de especificadores de portas.

Endereço IP

Um endereço especificado em uma das seguintes formas, opcionalmente precedido por um operador não:

qualquer

corresponde a qualquer endereço IP.

ip-numérico | hostname

Corresponde a um único endereço IPv4, especificado como quad-pontilhado ou um hostname. Nomes de host são resolvidos no momento em que a regra é adicionado à lista de firewall.

addr / bits

Um número de IP com uma máscara de largura da 1.2.3.4/24 formulário. Neste caso, todos os números IP de 1.2.3.0 a 1.2.3.255 irá corresponder.

addr: máscara

Um número de IP com uma máscara do formulário 1.2.3.4:255.255.240.0.
Neste caso, todos os números IP para from1.2.0.0 1.2.15.255 irá corresponder.

O sentido do jogo pode ser invertida se precedida por um endereço com o modificador não, fazendo com que todos os outros endereços, em vez de ser acompanhado. Isso não afeta a seleção de números de porta.

Portas: [,...]] porta: {porto | porto | porta-porta máscara} [,

O `- notação 'especifica um intervalo de portas (incluindo as fronteiras).

O `: a notação 'especifica uma porta e uma máscara, uma partida é declarada se o número da porta no pacote corresponde a um em regra, limitados aos bits que são definidos na máscara.

Os nomes de serviço pode ser utilizado em vez de valores numéricos porta.

Uma vasta só pode ser indicado como o primeiro valor, eo comprimento da lista de portas é limitado a 10 portas

Regra opções (padrões de jogo)

padrões de jogo adicionais podem ser usados dentro das regras. Zero ou mais dessas opções para chamadas podem estar presentes em uma regra.

> ipfw add 100 ip de não permitir a qualquer 1.2.3.4

Os padrões de correspondência a seguir podem ser utilizados (em ordem alfabética):

estabelecida

Jogos pacotes TCP que os bits RST ou ACK marcados.

fragmento

pacotes de jogos que são fragmentos e não o primeiro fragmento de um datagrama IP. Note-se que estes pacotes não terá o cabeçalho do protocolo próxima (por exemplo, TCP, UDP) para opções que olhar para estes cabeçalhos não podem igualar.

tipos icmptypes

ICMP ICMP jogos cujo tipo é na lista de tipos. A lista pode ser especificado como qualquer combinação de faixas de tipos individuais separados por vírgulas. O ICMP tipos suportados são:

echo reply (0), o destino inalcançável (3) fonte têmpera, (4), redirecionar

(5), solicitação de eco (8), anúncio de roteador (9), solicitação do roteador (10), time-to-live ultrapassado (11) , o cabeçalho IP 12), data e hora do pedido (ruim (13), a resposta timestamp (14), pedido de informações (15), a resposta de informações (16), a máscara de solicitação de endereço (17) e uma máscara de endereço de resposta (18).

in | out

Jogos pacotes de entrada ou saída, respectivamente. .

ipoptions spec

pacotes de jogos cujo cabeçalho IP contém a lista separada por vírgula de opções especificadas na especificação. As opções IP suportados são: SSRR (via fonte estrito), LSRR (rota de origem livre), RR (rota do pacote de registro) e TS (timestamp). A ausência de uma determinada opção pode ser denotado com um "!".

manter o estado-

Após uma partida, o firewall irá criar uma regra dinâmica, cujo comportamento é padrão para coincidir com o tráfego bidirecional entre origem e destino IP / porta usando o mesmo protocolo. A regra tem uma duração limitada, ea vida é atualizado a cada vez que um pacote for encontrado.

limite {src-addr | src-port | dst-addr | dst-port} N

O firewall só permita conexões N com o mesmo conjunto de parâmetros, conforme especificado na regra. Um ou mais endereços de origem e destino e portas podem ser especificadas.

recv | xmit | via {IFX | Se * | ipno | any}

Jogos pacotes recebidos, transmitidos ou passando, respectivamente, a interface especificada por pelo nome do dispositivo (caso *), por endereço IP ou através de alguma interface.

A via palavra-chave faz com que a interface para ser sempre verificado. Se recv ou xmit é usado em vez da via, então, apenas a receber ou transmitir interface (respectivamente) está marcada. Ao especificar ambos, é possível combinar pacotes com base em receber e transmitir interface, como por exemplo:

> ipfw add negar ip from any to any out ppp1 xmit recv eth1

A interface recv pode ser testado em um ou saída pacotes de entrada, enquanto a interface xmit só pode ser testado em pacotes de saída. Tão fora é necessário (e é inválido) xmit sempre é usado.

configuração

Pacotes TCP Jogos que possuem o bit SYN, mas nenhum bit ACK. Esta é a forma abreviada de syn tcpflags ``,!''Ack.

tcpflags spec

apenas os pacotes TCP. Menor se o cabeçalho TCP contém a lista separada por vírgula dos sinalizadores especificados na especificação. O TCP flags suportadas são:

fin, SYN, RST, ACK PSH e URG. A ausência de um pavilhão especial, podem ser indicadas por um `! '. Uma regra que contém uma especificação tcpflags nunca pode corresponder a um pacote fragmentado que tem um não-zero offset. Veja a opção frag para obter detalhes sobre harmonização pacotes fragmentados.

tcpoptions spec

apenas os pacotes TCP. Menor se o cabeçalho TCP contém a lista separada por vírgula de opções especificadas na especificação. O TCP opções suportadas são:

MSS (tamanho máximo do segmento), janela (tcp propaganda janela), saque (confirmação seletiva), TS (RFC1323 timestamp) e cc (rfc1644 t / contagem conexão TCP). A ausência de uma determinada opção pode ser denotado com um "!".

Checklist

Aqui estão alguns pontos importantes a considerar na elaboração de suas regras:

- Lembre-se que você filtre os pacotes entrando e saindo. A maioria das conexões necessidade pacotes indo em ambas as direções.
- Lembre-se de teste muito cuidado. É uma boa idéia para estar perto do console quando está fazendo isso.
- Não esqueça o interface loopback.

firewall Stateful

Stateful operação é uma forma de o firewall dinamicamente criar regras para fluxos específicos quando os pacotes que correspondem a um determinado padrão são detectados. Suporte para operação stateful vem a verificar, manter o estado eo estado limite de opções por meio de regras.

regras dinâmicas são criadas quando um pacote corresponde a um estado de manter ou regra do limite, fazendo com que a criação de uma regra dinâmica, que irá corresponder a todos e somente os pacotes com um determinado protocolo entre um dst-ip/dst-port src-ip/src-port par de endereços (src e dst são usados aqui apenas para indicar os endereços de partida inicial, mas eles são completamente equivalentes depois). regras dinâmicas serão verificados na primeira seleção do Estado, manter o estado ou limitar a ocorrência ea ação realizada em cima de um jogo será o mesmo que a regra principal.

Note que não há outros atributos que não o protocolo e endereços IP e os portos são controlados sobre as regras dinâmicas.

O uso típico de regras dinâmicas é manter uma configuração de firewall fechado, mas que o primeiro pacote TCP SYN da rede dentro de instalar uma regra dinâmica para o fluxo, de modo que os pacotes que pertencem a essa sessão será permitido através do firewall:

```
ipfw add check-estado
ipfw add permitir que o TCP do meu sub-rede para todo o estado setup keep-
ipfw add negar tcp from any to any
```

Uma abordagem semelhante pode ser usado para UDP, onde um pacote UDP que vem do interior irá instalar uma regra dinâmica para permitir que a resposta através do firewall:

```
ipfw add check-estado
ipfw add permitir udp da minha sub-rede para manter qualquer estado
ipfw add negar udp from any to any
```

Regras dinâmicas expirar após algum tempo, que depende do estado do fluxo.

Veja EXEMPLOS Secção de mais exemplos de como usar as regras dinâmicas.

Exemplos

Há demasiadas possíveis utilizações do ipfw que esta secção só vai dar um pequeno conjunto de exemplos.

Básico de filtragem de pacotes

Este comando adiciona uma entrada que nega todos os pacotes TCP de cracker.evil.org à porta telnet de wolf.tambov.su sejam encaminhados pelo anfitrião:

```
ipfw add negar TCP cracker.evil.org telnet wolf.tambov.su
```

Este não permite qualquer conexão da rede crackers toda a minha host:

```
ipfw add nega IP de 123.45.67.0/24 para my.host.org
```

A primeira maneira eficiente e para limitar o acesso (não usando regras dinâmicas) é a utilização das seguintes regras:

```
ipfw add permitir tcp from any to any estabelecido
ipfw add permitir que o TCP de net1 portlist1 para NET2 portlist2
configuração
ipfw add permitir que o TCP de net3 portlist3 para net3 portlist3
configuração
...
ipfw add negar tcp from any to any
```

A primeira regra será uma partida rápida de pacotes TCP normal, mas não vai combinar o pacote SYN inicial, que será acompanhado pelas regras de instalação somente para a fonte selecionada destino pares /. Todos os outros pacotes SYN será rejeitado pela regra de negação final.

regras dinâmicas

A fim de proteger um site de ataques de inundação de pacotes TCP envolvendo falsos, é mais seguro usar regras dinâmicas:

```
ipfw add check-estado
ipfw add negar tcp from any to any estabelecido
ipfw add permitir que o TCP do meu-net para todo o estado setup keep-
```

Isso permitirá que o firewall instalar regras dinâmicas somente para aqueles que começam conexão com um pacote SYN regular vindo de dentro da nossa rede. regras dinâmicas são verificados quando se deparam com o primeiro verificar o estado ou a regra do estado se manter. Um estado de regras de seleção devem ser normalmente colocados perto do início do conjunto de regras para minimizar a quantidade de trabalho de digitalização do conjunto de regras.

Para limitar o número de conexões que um usuário pode abrir você pode usar os seguintes tipos de regras:

```
ipfw add permitir que o TCP de my-net/24 a qualquer limite de instalação
addr-src 10
ipfw add permitir tcp from any to me limitar a instalação addr-src 4
```

O primeiro (supondo que é executado em um gateway) que permitirá a cada host em uma rede / 24 para abrir mais de 10 conexões TCP. Este último pode ser colocado em um servidor para se certificar de que um único cliente não usa mais de 4 conexões simultâneas.

CUIDADO: regras stateful pode ser objecto de negação de serviço ataques por inundação SYN, que abre um enorme número de regras dinâmicas.

Esta regra gotas aleatórias pacotes de entrada com uma probabilidade de 5%:

```
ipfw add prob 0,05 negar ip from any to any em
```

Aqui está uma boa utilização do comando list para ver os registros contábeis e informações timestamp:

```
ipfw-na lista
```

ou na forma abreviada, sem timestamps:

```
ipfw uma lista
```

que é equivalente a:

```
ipfw show
```

Veja também

S. Floyd e V. Jacobson, Detecção Precoce gateways aleatórios para Evitar Congestionamento, agosto de 1993.

B. Braden, D. Clark, J. Crowcroft, B. Davie, S. Deering, D. Estrin, S. Floyd, V. Jacobson, G. Minshall, C. Partridge, L. Peterson, K. Ramakrishnan, S. Shenker, J. Wroclawski, e L. Zhang, recomendações sobre a gestão da fila e evitar o congestionamento na Internet, Abril de 1998, RFC 2309.

Atenção!

Misconfiguring o firewall pode colocar seu computador em um estado inutilizável, possivelmente, encerrar os serviços de rede e exigindo acesso ao console de recuperar o controle para ele.

Autores

- JS Ugen Antsilevich
- Poul-Henning Kamp
- Alex Nash
- Archie Cobbs
- Luigi Rizzo

API baseada em código escrito por Daniel Boulet para BSDI.

IPFW portado para Windows ® por Ruslan Goncharov Staritsin e Vladislav.

WIPFW projecto de 2005