Firewall
Tecnologia de Filtragem

Matteo Nava
Adilson Eduardo Guelfi
Volnys Bernal

LSI - Laboratório de Sistemas Integráveis
Escola Politécnica da USP

PROCESSO DE FILTRAGEM

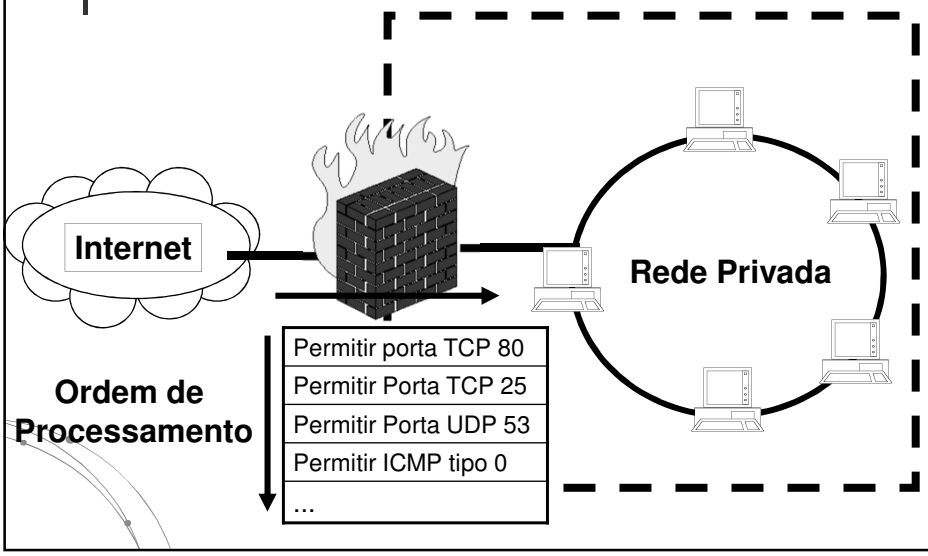
3

Filtragem de pacotes

- **Funcionamento:**
  - Baseia-se na filtragem de datagramas IP recebidos, através de decisões do tipo “permitir/bloquear”
  - Cada decisão “permitir/bloquear” é tomada consultando-se as regras de filtragem estabelecidas e os cabeçalhos TCP/IP do datagrama
- **Exemplos de regras de Filtragem:**
  - **“Permitir Telnet somente para IP 143.107.161.199”**
  - **“Repudiar todas as mensagens ICMP externas”**

4

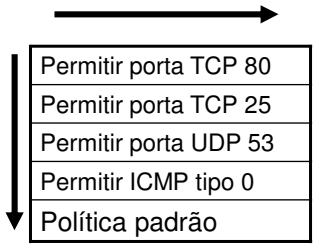
Filtragem de pacotes



5

Processo de análise

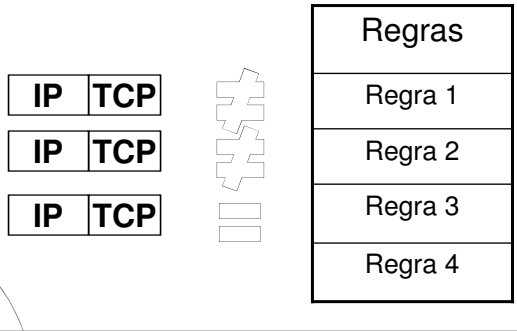
- Cada datagrama em transito é comparado com as regras de filtragem definidas
- As regras de filtragem são varridas de forma sequencial, de cima para baixo
- Quando um datagrama satisfaz uma regra há um *Match* e sai da fila
- A listagem das regras termina com a política padrão



6

Filtragem de pacotes

- Controle de acesso baseado na comparação do cabeçalho do pacote com as regras de filtragem

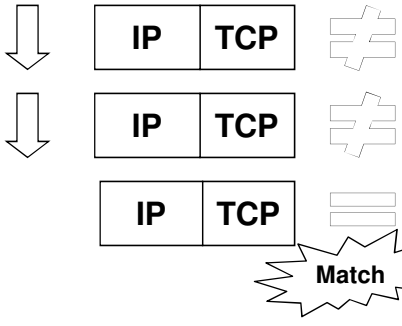


7

Match do datagrama

- **O Match se da quando todos os parâmetros definidos na regras são satisfeitos**

S: 10.0.0.5 D: 192.168.0.12	TCP Porta S: 5420 Porta D: 80



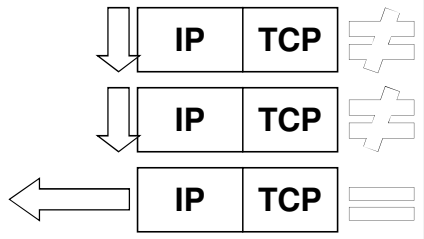
Regra
Protocolo TCP Porta 80 IP S: 192.168.0.0/16
Protocolo UDP Porta 80
Protocolo TCP Porta 80
Protocolo ICMP Tipo 8

8

Ação correspondente ao Match

S: 10.0.0.5 D: 192.168.0.12	TCP Porta S: 5420 Porta D: 80

Cabeçalho recebido



Pacote aceito
Acesso permitido

Regra	Ação
Protocolo TCP Porta 25	Permitido
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Protocolo ICMP Tipo 8	Negado
....	...

9

Política padrão

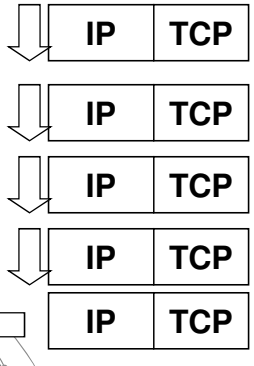
- **A Política padrão se aplica quando um datagrama não realiza nenhum Match com as regras definidas**
  - Padrão = Descartar tudo
    - Para políticas de controle mais restritivas
    - Tudo que não é expressamente permitido é proibido
    - Necessário definir regras para permitir tráfego desejado
  - Padrão = Aceitar tudo
    - Para políticas mais permissivas
    - Tudo que não é expressamente proibido é permitido
    - Devem ser definidas regras para bloquear tráfego indesejado

10

Política padrão

S: 10.0.0.5 **D: 192.168.0.12**	**TCP**	**Porta S: 5420** **Porta D: 137**

Cabeçalho recebido



Acesso negado

Regra	Acesso
Protocolo TCP Porta 25	Permitido
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Protocolo ICMP Tipo 8	Negado
Any:any	Negado

Considerações

- A regras estão em uma única tabela
- A tabela é varrida em uma direção (p. ex. de cima para baixo)
- Quando houver um match o pacote sai da fila de processamento
- A ordem das regras é muito importante pois regras iguais mas com ordem diferente podem gerar resultados diferentes

Importância da ordem das regras

Conjunto 1

Regra	Acesso
Protocolo TCP Porta 25	Permitido
IP S:10.0.0.0/24	Negado
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Padrão	Negado

Conjunto 2

Regra	Acesso
IP S:10.0.0.0/24	Negado
Protocolo TCP Porta 25	Permitido
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Padrão	Negado

S: 10.0.0.5 **D: 192.168.0.12**	**TCP**	**Porta S: 5420** **Porta D: 25**

Cabeçalho recebido

13

Importância da ordem das regras

S: 10.0.0.5 D: 192.168.0.12	TCP Porta S: 5420 Porta D: 25

Cabeçalho recebido

Acesso Permitido

Conjunto 1

Regra	Acesso
Protocolo TCP Porta 25	Permitido
IP S:10.0.0.0/24	Negado
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Padrão	Negado

14

Importância da ordem das regras

S: 10.0.0.5 D: 192.168.0.12	TCP Porta S: 5420 Porta D: 25

Cabeçalho recebido

Acesso negado

Conjunto 2

Regra	Acesso
IP S:10.0.0.0/24	Negado
Protocolo TCP Porta 25	Permitido
Protocolo UDP Porta 53	Permitido
Protocolo TCP Porta 80	Permitido
Padrão	Negado

15

Otimização das regras

Cada linha da tabela de regras demanda uma etapa de processamento (ciclos de CPU do firewall)

- **Muito importante otimizar as regras:**
  - Ajustando a ordem
  - Consolidando as regras de forma eficiente

16

GERENCIAMENTO DO ESTADO

Gerenciamento do fluxo de comunicação

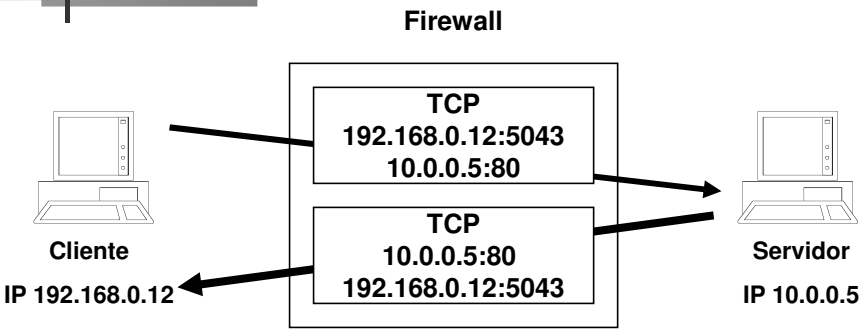
- **Tecnologias para gerenciamento do fluxo:**
  - **Stateless: Sem conhecimento do estado**
  - **Stateful: com conhecimento do estado**

Tecnologia Stateless

- **Cada pacote é analisado individualmente**
- **Não há conhecimento do estado da comunicação**
- **Tecnologia antiga e em desuso**
- **Desvantagem**
  - Impossibilidade de implementação de regras precisas
  - Complexidade das regras de filtragem
  - Dificuldade de gerenciamento de regras de filtragem
    - A cada regra de entrada precisa definir uma regra de saída
    - A regra de saída é excessivamente permissiva

19

Stateless



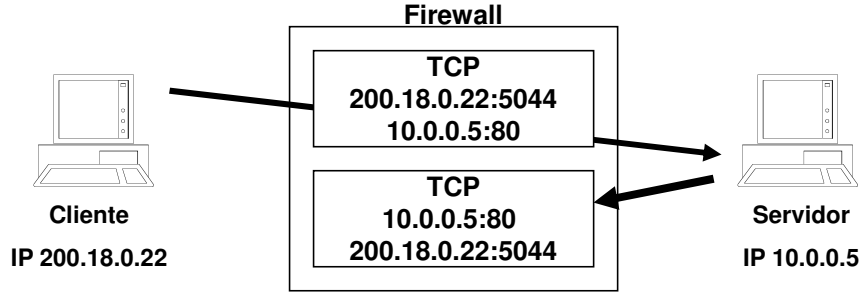
Quantas regras são necessárias?

	IP origem	Porta Origem	IP destino	Porta Destino	Ação
Regra de entrada	Any	➢1023	10.0.0.5	TCP 80	Aceita
Regra de saida	10.0.0.5	80	192.168.0.12	5043	Aceita

20

Stateless

A regra definida atende a esta nova requisição?



	IP origem	Porta Origem	IP destino	Porta Destino	Ação
Regra de entrada	Any	➢1023	10.0.0.5	TCP 80	Aceita
Regra de saida	10.0.0.5	80	192.168.0.12	5043	Aceita

Stateless – regras genéricas

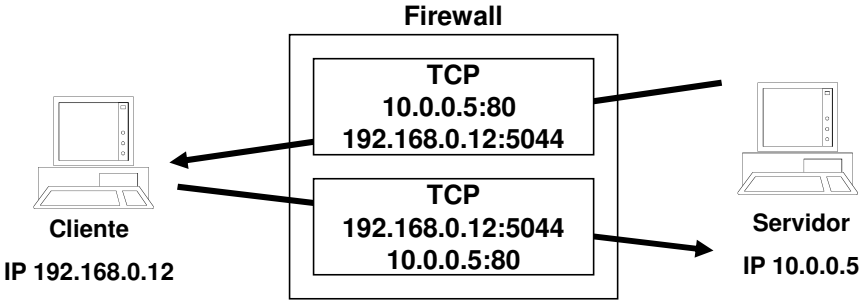
Precisa gerar regras suficientemente genéricas para permitir a volta a todas as origens

	IP origem	Porta Origem	IP destino	Porta Destino	Ação
Regra de entrada	Any	➢1023	10.0.0.5	TCP 80	Aceita
Regra de saida	10.0.0.5	80	Any	➢1023	Aceita

Para garantir o fluxo de retorno precisa habilitar:
- **Qualquer destino**
- **As portas altas >1023**

Stateless - Problema de Segurança

Pois não ha controle sobre a direção do fluxo de comunicação, as regras definidas permitem fluxos não previstos

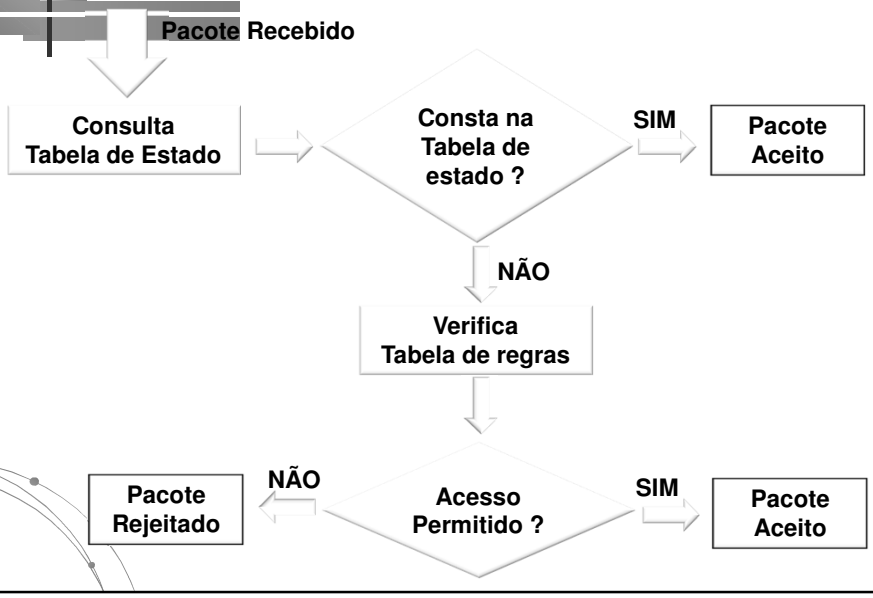


IP origem	Porta Origem	IP destino	Porta Destino	Ação
Any	➢1023	10.0.0.5	TCP 80	Aceita
10.0.0.5	80	Any	➢1023	Aceita

Tecnologia Stateful

- **Utiliza uma tabela de estado que mantêm o estado de cada "fluxo de comunicação"**
- **Os pacotes são analisados como componentes de um único fluxo de dados, permitindo uma análise mais eficiente e rápida**
- **Fluxo de análise:**
  - Para cada pacote recebido é verificado se há correspondência na tabela de estado
  - Caso não haja, é verificada a lista de controle de acesso

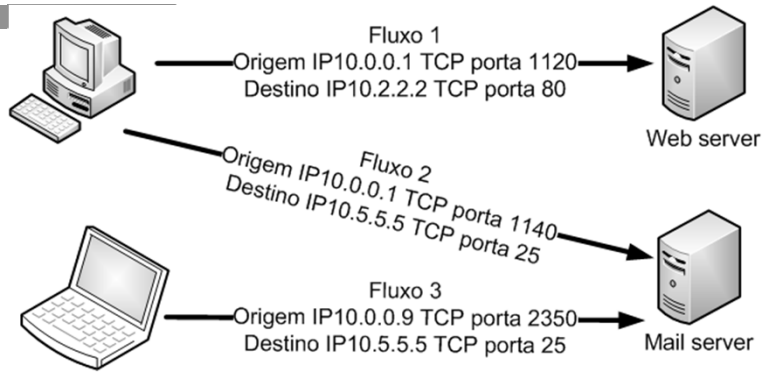
Fluxo de análise com tabela de estado



Stateful - Tabela de estado

- Tabela dinâmica utilizada para realizar o *track* (rastreamento) das comunicações
- Cada nova conexão aceita gera uma nova entrada na tabela
- A validação do pacote (filtragem) é aplicada somente ao primeiro pacote do fluxo pertencente a comunicação

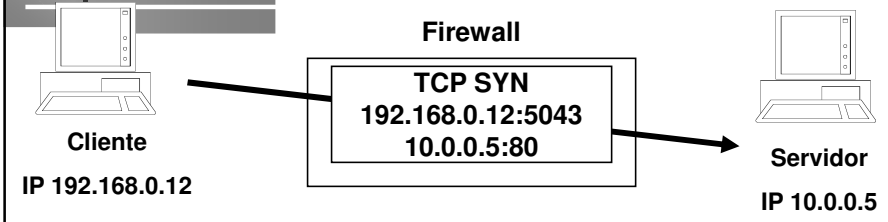
Tabela de estado



IP origem	Porta origem	IP destino	Porta destino	Estado
10.0.0.1	1120	10.2.2.2	80	NEW
10.0.0.1	1140	10.5.5.5	25	ESTABLISHED
10.0.0.9	2350	10.5.5.5	25	ESTABLISHED

27

Tecnologia Stateful - Funcionamento



1º Verifica Tabela de estado

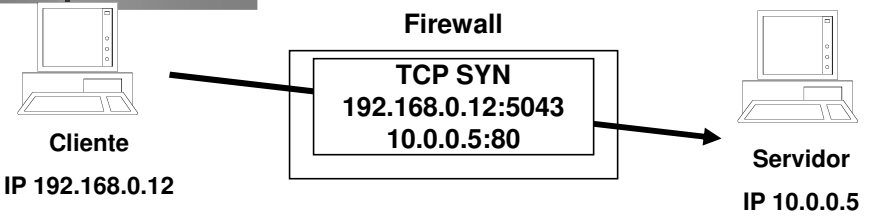
IP Origem	Porta Origem	IP destino	Porta destino
200.1.0.12	2598	10.0.0.5	80
189.21.2.54	6789	10.0.0.5	80

2º Verifica regras de firewall

IP Origem	Porta Origem	IP destino	Porta Destino	Ação
ANY	>1023	10.0.0.5	80	Permitido

28

Tecnologia Stateful - Funcionamento

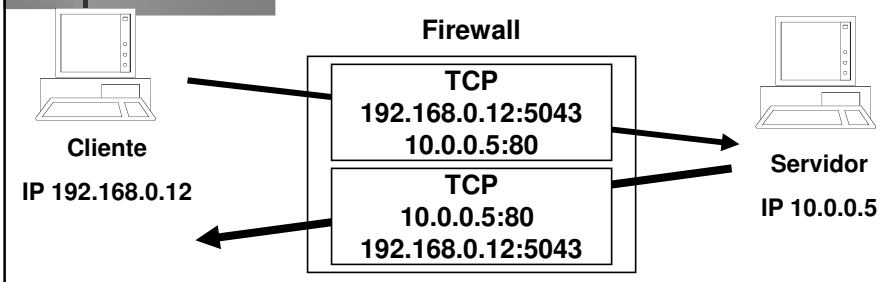


3º se a comunicação for aceita, é inserido um novo registro de comunicação na Tabela de estado

IP Origem	Porta Origem	IP destino	Porta destino
200.1.0.12	2598	10.0.0.5	80
189.21.2.54	6789	10.0.0.5	80
192.168.0.12	5043	10.0.0.5	80

29

Tecnologia Stateful - Funcionamento



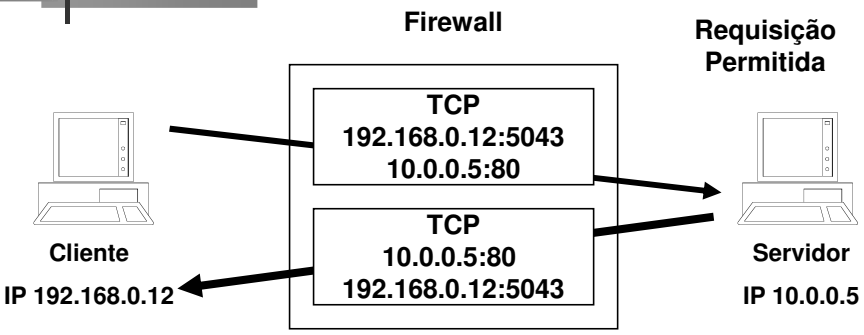
4º o retorno da comunicação é permitido consultando a tabela de estado

IP Origem	Porta Origem	IP destino	Porta destino
192.168.0.12	5043	10.0.0.5	80

5º também a passagem dos outros pacotes do mesmo fluxo é permitida utilizando a tabela de estado

30

Tecnologia Stateful

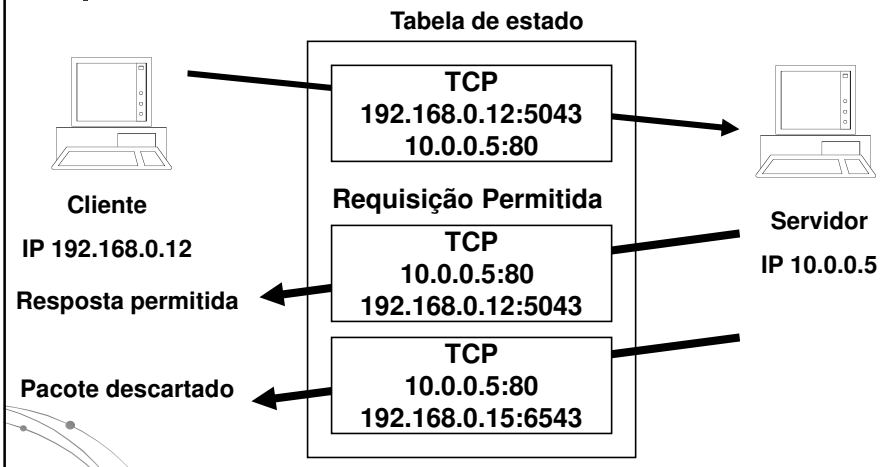


Quantas regras são necessárias?

IP Origem	Porta Origem	IP destino	Porta Destino	Ação
ANY	>1023	10.0.0.5	80	Permitido

31

Tecnologia Stateful - segurança



32

CRIAÇÃO DE REGRAS

Criação de regras de firewall

- **Necessidade apresentada:**
  - Permitir acesso da Internet ao servidor Web de e-commerce
- **Estudo da necessidade de acesso:**
  - Acesso serviços http e https nas portas TCP 80 e 443
  - Acesso IP do servidor Web 10.0.10.12
  - Acesso permitido para qualquer sistema na Internet
- **Formalização das regras de acesso:**

IP origem	Porta Origem	IP destino	Porta Destino	Ação
Any	TCP > 1023	10.0.10.12	TCP 80	Aceita
Any	TCP > 1023	10.0.10.12	TCP 443	Aceita