

Segurança de Dados

Firewalls

MSc. Danilo Lucena
danilocglucena@gmail.com



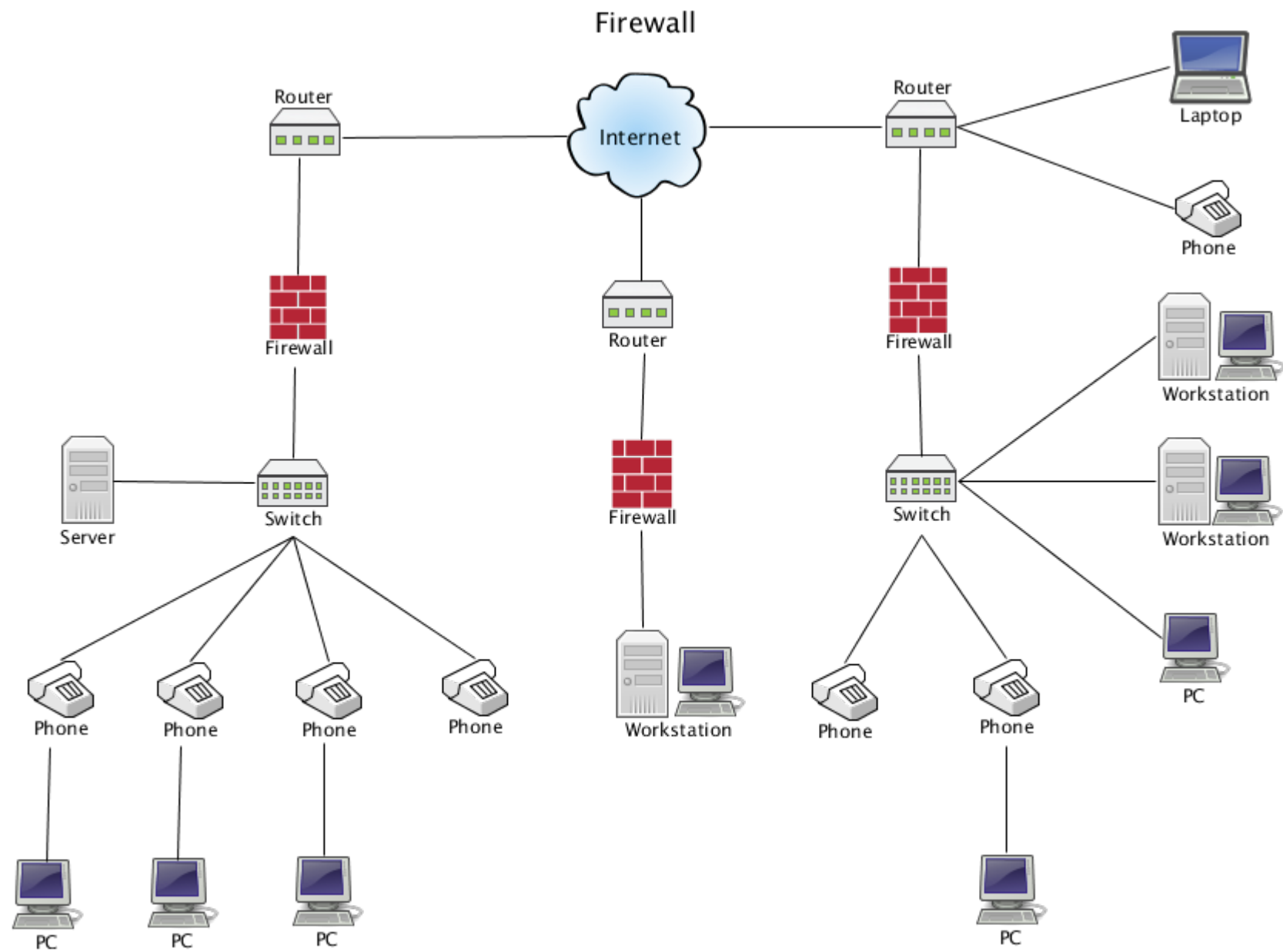
Material

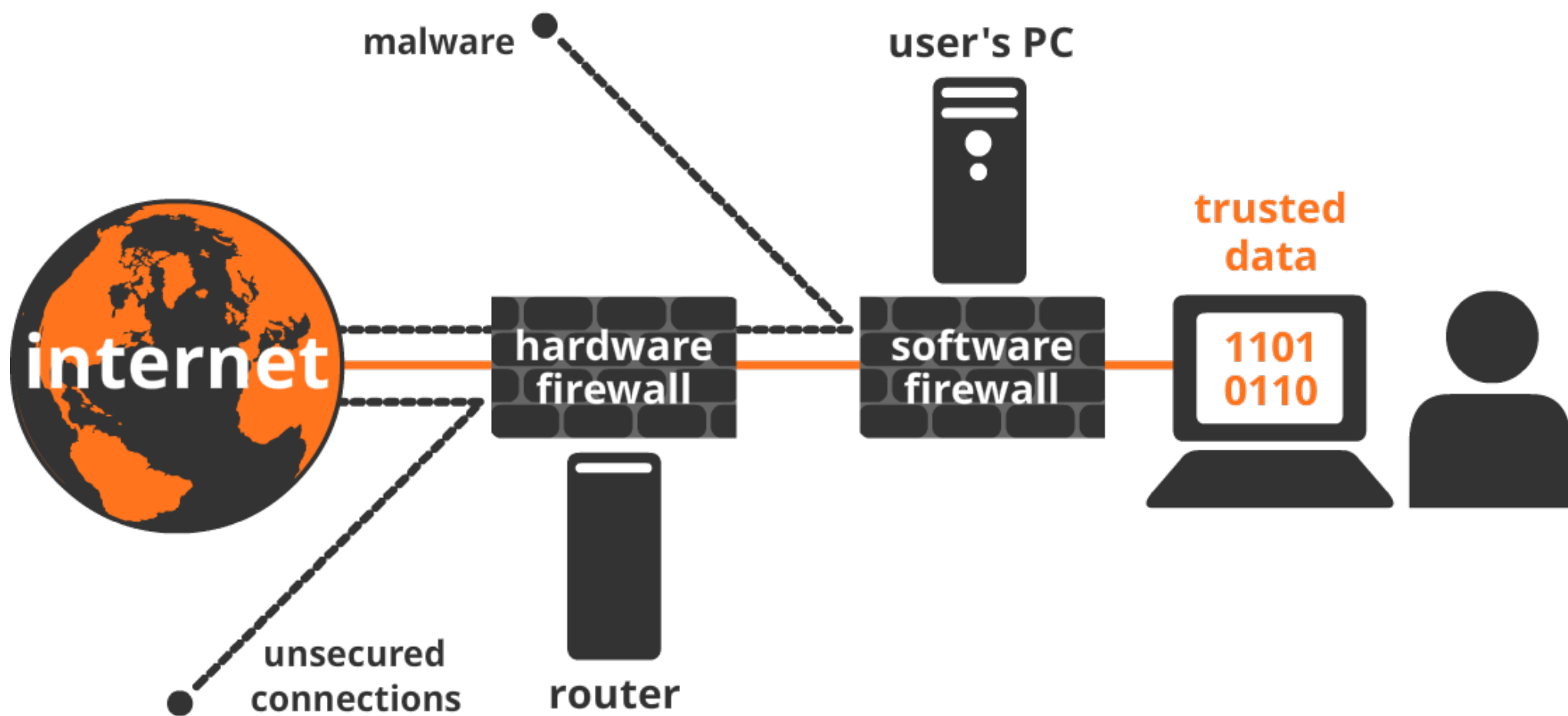
- Livro base “Introdução a Segurança de Computadores”.
- Capítulo 06.
- Versão em inglês ou português (iguais).

Introdução

Introdução

- Com a crescente adoção da Internet como meio principal de tráfego de dados, também aumentou a quantidade de programas maliciosos.
 - Vírus;
 - Exploits;
 - Espionagem;
- Uma das formas de “garantir” uma segurança mínima em redes locais ou em máquinas individuais é o uso de **firewall**.





Introdução

- Firewalls podem utilizadas como medidas protetivas, para isolar uma rede de ataques maliciosos da Internet.
- Ou pode ser usado como ferramenta de censura, com o objetivo de limitar o acesso a determinados conteúdos.
 - Redes corporativas com restrição de acesso.
 - Controle parental de conteúdo sensível.
 - Controle governamental.

The Great Firewall of China

Bloomberg News

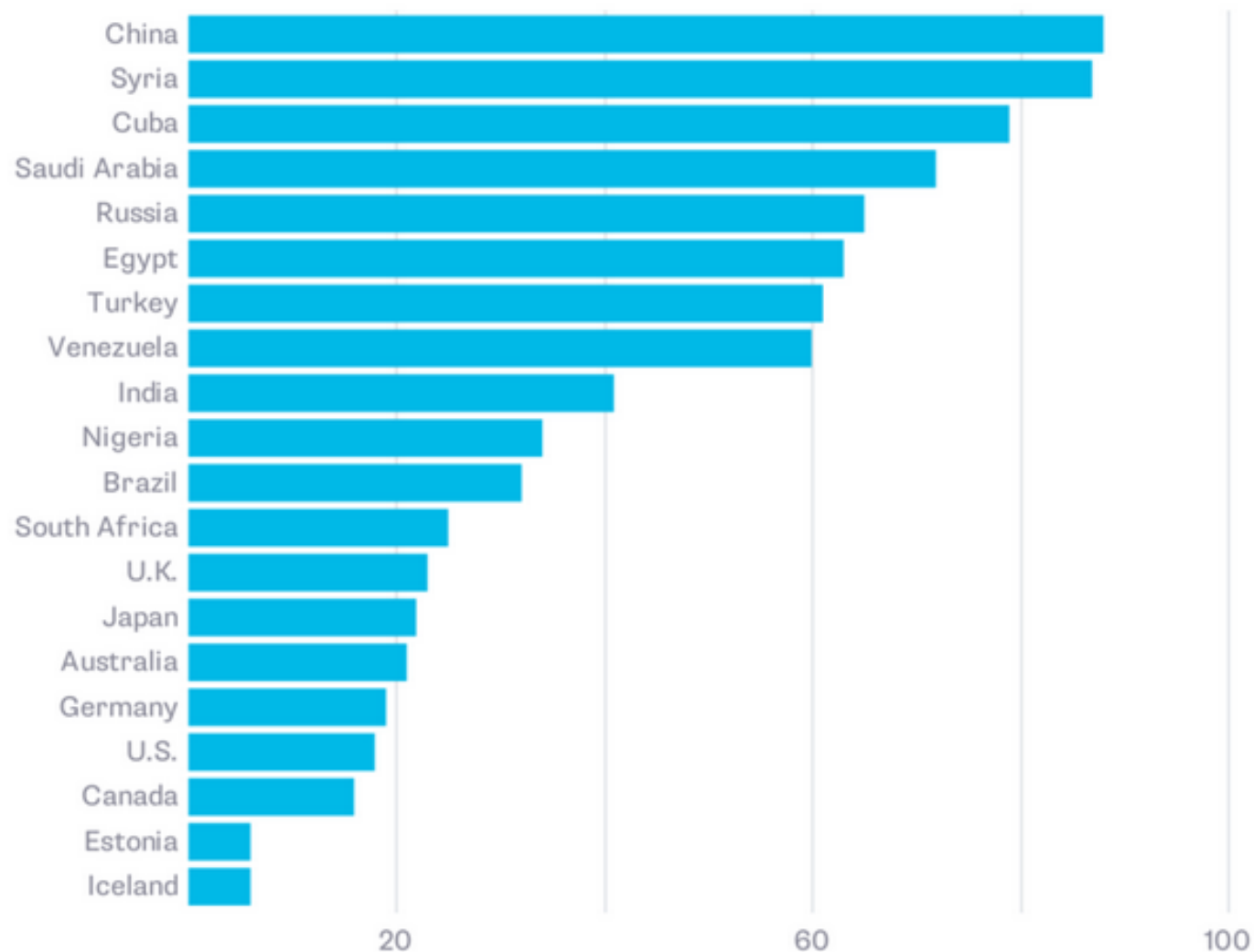
Updated on December 1, 2017, 12:19 AM GMT-3

From **Bloomberg QuickTake**

China's online population of 731 million gets a highly restricted internet, one that doesn't include access to Google, Facebook, YouTube or the New York Times. There's little coverage of the 1989 student protests in Tiananmen Square. Even Winnie the Pooh got temporarily banned. China is able to control such a vast ocean of content through the largest system of censorship in the world, aptly known as the Great Firewall of China. It's a joint effort between government monitors and the technology and telecommunications companies that are compelled to enforce the state's rules. The stakes go beyond China, which is setting an example that other authoritarian countries can imitate.

World's Worst for Online Freedom? China Edges Syria

Iceland, Estonia come out best in Freedom House's rankings



Note: Rankings are for 2016; score of 0 is most free, 100 least free

BloombergQuickTake

A Stanford Project

[← Within the Wall : Perceptions of Censorship by the Average Chinese Netizen](#)

[The Great Firewall: a technical perspective →](#)

The Great Firewall of China: Background

Posted: June 1, 2011 | **Author:** [pingp](#) | **Filed under:** [Great Firewall of China](#) | [Leave a comment »](#)

The Great Firewall of China, also formally known as the Golden Shield Project, is the Chinese government's internet censorship and surveillance project. Initiated, developed, and operated by the Ministry of Public Security (MPS), the project is one of the most controversial subjects in the world. While many people of the Western world treat the project as a human right violation, some countries are actually adopting China's model. Some people think that the issue is interesting because the Chinese economy benefits tremendously from the Internet, but the Internet, in turn, is interfering with its political stability. Other people think that it is just a matter of time until Chinese communism collapses. On this website, we will provide a thorough examination of historical and technical aspects of the Great Firewall of China.

Firewall

- Um firewall é um conjunto de tecnologias, implementadas em software ou hardware que são colocados nos pontos de saída da interface de rede de um computador ou no perímetro de saída de uma rede local.
- Como prerrogativa, considera-se que toda a comunicação com a Internet representa um perigo em potencial.
 - Tudo o que está além do firewall = inseguro.
 - Tudo o que está dentro da zona do firewall = seguro.
 - Qual a diferença para um SO ou admin de rede?

Firewall - policies

- Conceitualmente, todas as tecnologias que compõem um firewall são organizados em termos de permissões ou de políticas de acesso.
- Cada pacote que passa pelo firewall recebe um status de alerta:
 - Aceito – os dados podem passar pelo firewall.
 - Desistente – os dados não possuem permissão.
 - Rejeitado – além de barrar os dados, dispara um alerta.

Firewall - policies

- Internamente, um firewall faz uma análise dos pacotes de dados.
- Realiza uma inspeção no seu conteúdo.
- Utiliza heurísticas (regras) para a análise.
 - Tipo do pacote (TCP, UDP);
 - Endereço IP de destino;
 - Portas;
 - Payload do pacote (existe vírus?).

What about powerful blocking mechanisms?

An adversary with a great deal of manpower and money, and severe real-world penalties to discourage people from trying to evade detection, is a difficult test for an anonymity and anti-censorship system.

The original Tor design was easy to block if the attacker controls Alice's connection to the Tor network --- by blocking the directory authorities, by blocking all the relay IP addresses in the directory, or by filtering based on the fingerprint of the Tor TLS handshake. After seeing these attacks and others first-hand, more effort was put into researching new circumvention techniques. Pluggable transports are protocols designed to allow users behind government **firewalls** to access the Tor network.

We've made quite a bit of progress on this problem lately. You can read more details on the [pluggable transports page](#). You may also be interested in [Roger and Jake's talk at 28C3](#), or [Runa's talk at 44con](#).

I'm behind a NAT/Firewall.

See <http://portforward.com/> for directions on how to port forward with your NAT/router device.

If your relay is running on a internal net you need to setup port forwarding. Forwarding TCP connections is system dependent but the firewalled-clients FAQ entry offers some examples on how to do this.

Also, here's an example of how you would do this on GNU/Linux if you're using iptables:

```
/sbin/iptables -A INPUT -i eth0 -p tcp --destination-port 9001 -j ACCEPT
```

You may have to change "eth0" if you have a different external interface (the one connected to the Internet). Chances are you have only one (except the loopback) so it shouldn't be too hard to figure out.

FreeProxy / FreeWeb

Define / Change Port Redirection

Name :

Protocol :

Client Port :

Local binding : Any IP address

Remote binding : Any IP address


Use Proxy Server ? ☐

Proxy Server

Read Timeout (seconds) :

Connect Timeout (seconds) :

Report all connects ? ☐

Log File : 

Calendar :

Demand Dial :

HTTP Options

☐ Use PASV with FTP over HTTP ?

☐ Use HTTP Authentication ?

Authentication Challenges:

☒ Basic

☐ Digest

☐ NTLM

Permissions...

Delete Cancel Done

Firewall - policies

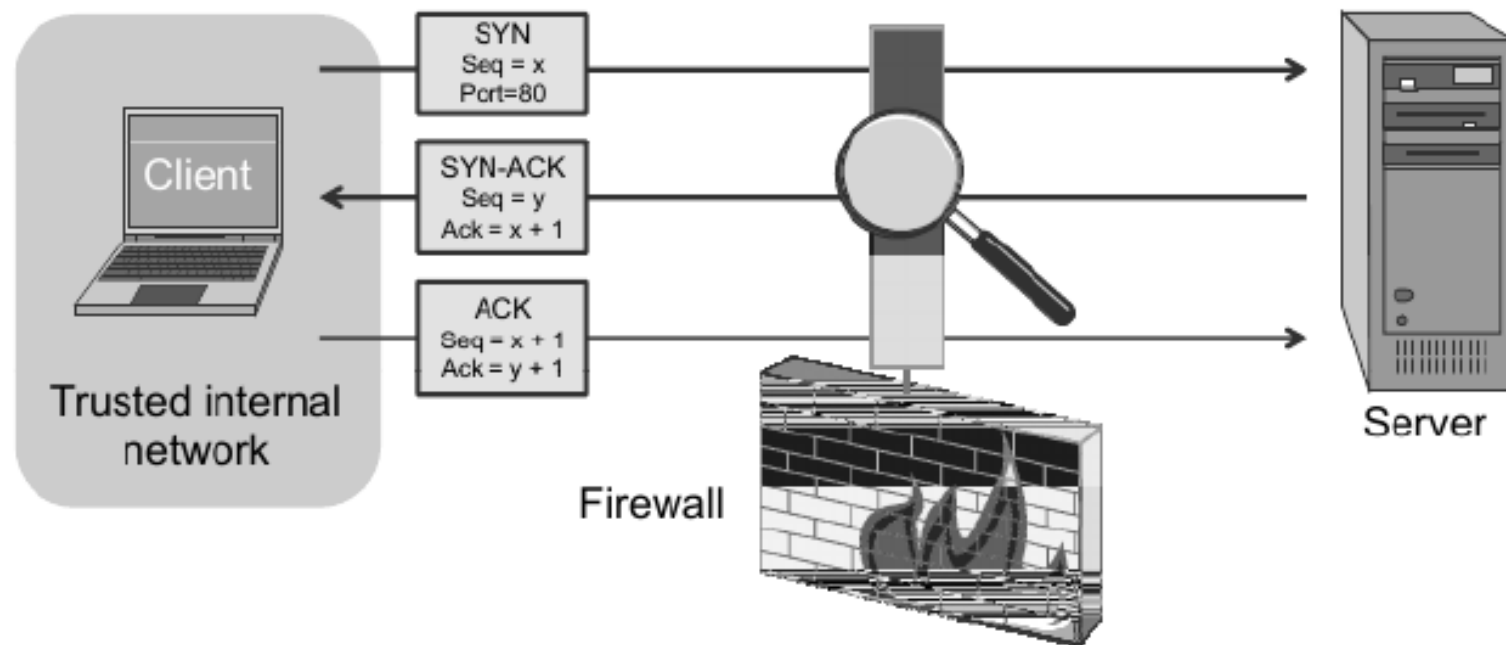
- Policies ou Rule sets.
- As regras de firewall servem para garantir quais partes da rede (local) ou tipos de pacotes são seguros ou quais devem ser colocados sob análise.
- Uma abordagem possível é a criação de **blacklists**.
 - Todos os pacotes são permitidos;
 - Exceto os pacotes com características da blacklist.
 - Retidos para análise ou bloqueados automaticamente.

Firewall - policies

- Blacklists simplificam a implementação e atuação do firewall.
- Também ajuda a minimizar conflitos com novos serviços.
- A criação da blacklist é tarefa do administrador da rede.

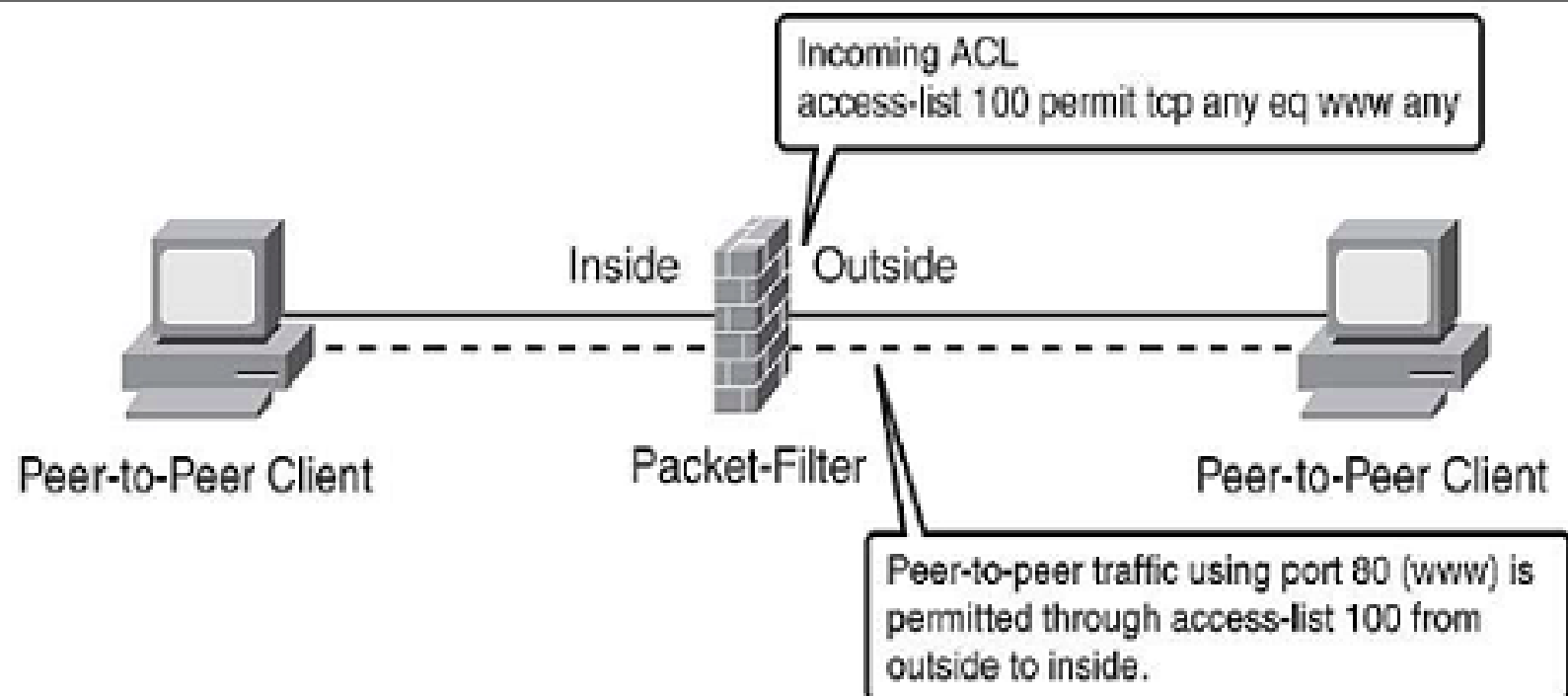
Firewall - Stateless

- Uma configuração padrão muito comum na utilização de firewalls.
- Sem estado, ou sem memorizar contextos.
- Ao analisar pacotes, não considera outros pacotes que podem ser enviados em conjunto.
- Cada pacote de forma isolada.
- Utiliza menos carga de processamento mas possuem uma atuação limitada (mecanismos conhecidos conseguem burlar essa configuração padrão).



Allow outbound SYN packets, destination port=80
Allow inbound SYN-ACK packets, source port=80

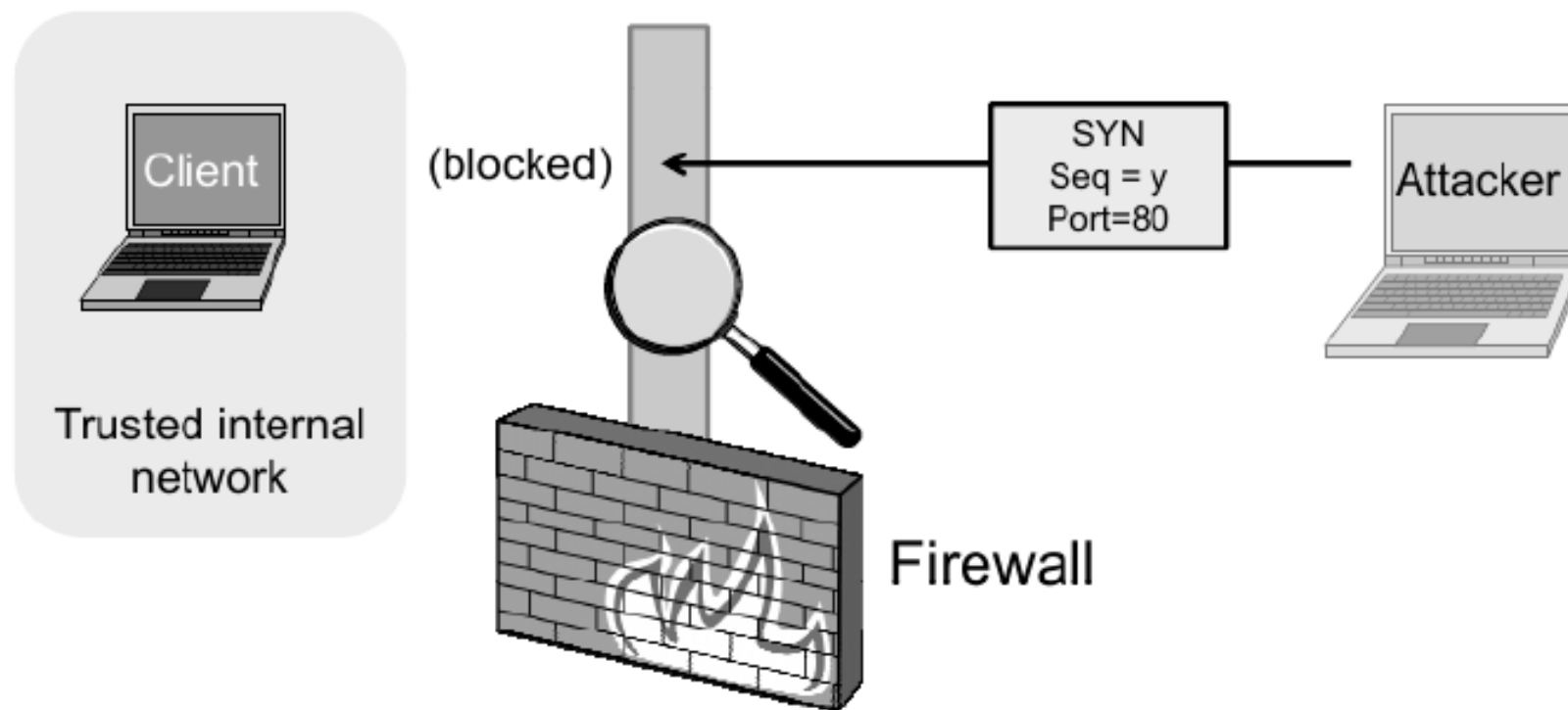
Figure 11: A stateless firewall allowing TCP sessions initiating an HTTP connection (port 80) with a request from the trusted internal network.



Stateless Packet Firewall

Firewall - Stateless

- Com essa configuração, é possível criar pontos de vulnerabilidade.
- Uma possibilidade para minimizar essa política menos restritiva é o uso de algum tipo de análise dos pacotes baseado em heurísticas conhecidas.
 - Ex. pacotes TCP com a flag SYN;
 - Pode evitar que pontos externos iniciem conexão.



Allow outbound SYN packets, destination port=80
Drop inbound SYN packets,
Allow inbound SYN-ACK packets, source port=80

Figure 12: A stateless firewall dropping TCP sessions initiating an HTTP connection with a request from outside the trusted internal network.

Firewall - Stateful

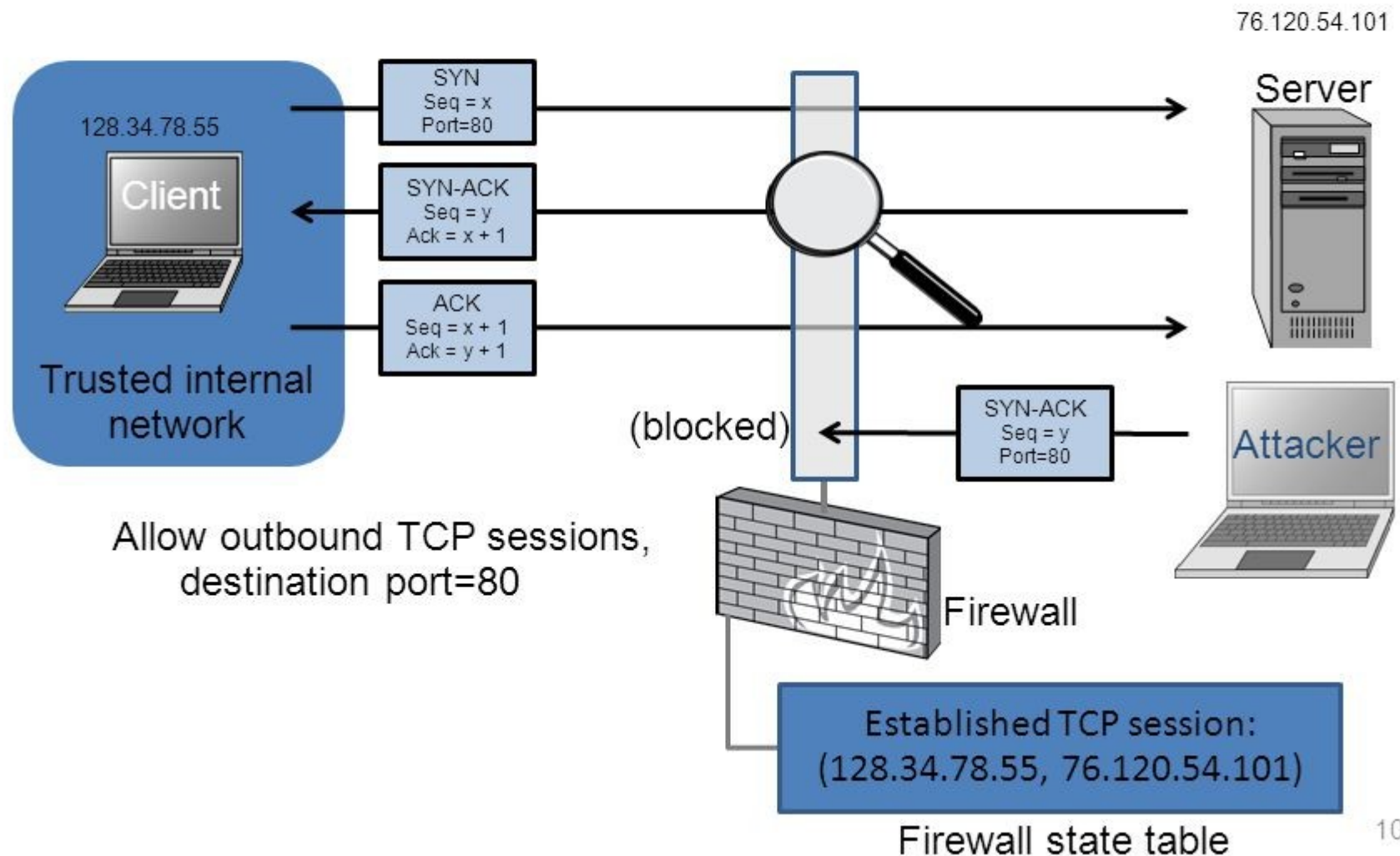
- A configuração no modo stateless não considera o tráfego anterior ao pacote que está sendo analisado pelo firewall.
- Não é possível determinar se um pacote é ou não uma resposta a um pacote anterior (que pode ser originário de um atacante).
- O modo de configuração stateful é o oposto.
- Pode identificar se um pacote faz parte de um processo de comunicação.
- Analisa o contexto geral da comunicação.

Firewall - Stateful

- São criadas tabelas contendo informações sobre cada uma das conexões ativas.
 - Endereços IP;
 - Portas;
 - Sequência numérica dos pacotes.
- Com essas tabelas, é possível impedir alguns tipos de ataques.
 - Impedir chegada de pacotes TCP;
 - Permitir apenas quando iniciadas internamente.

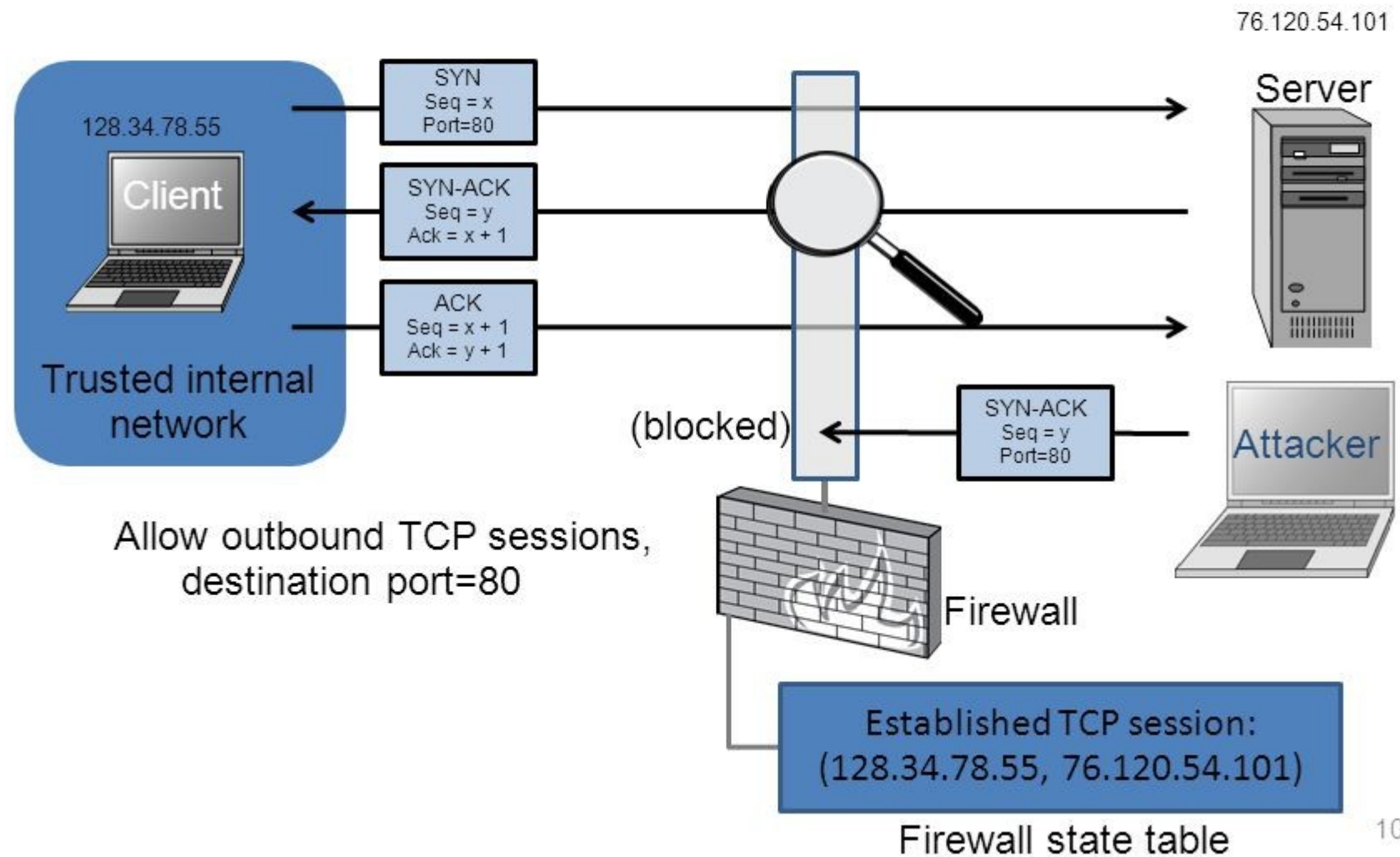
Stateful Firewall Example

- Allow only requested TCP connections:



Stateful Firewall Example

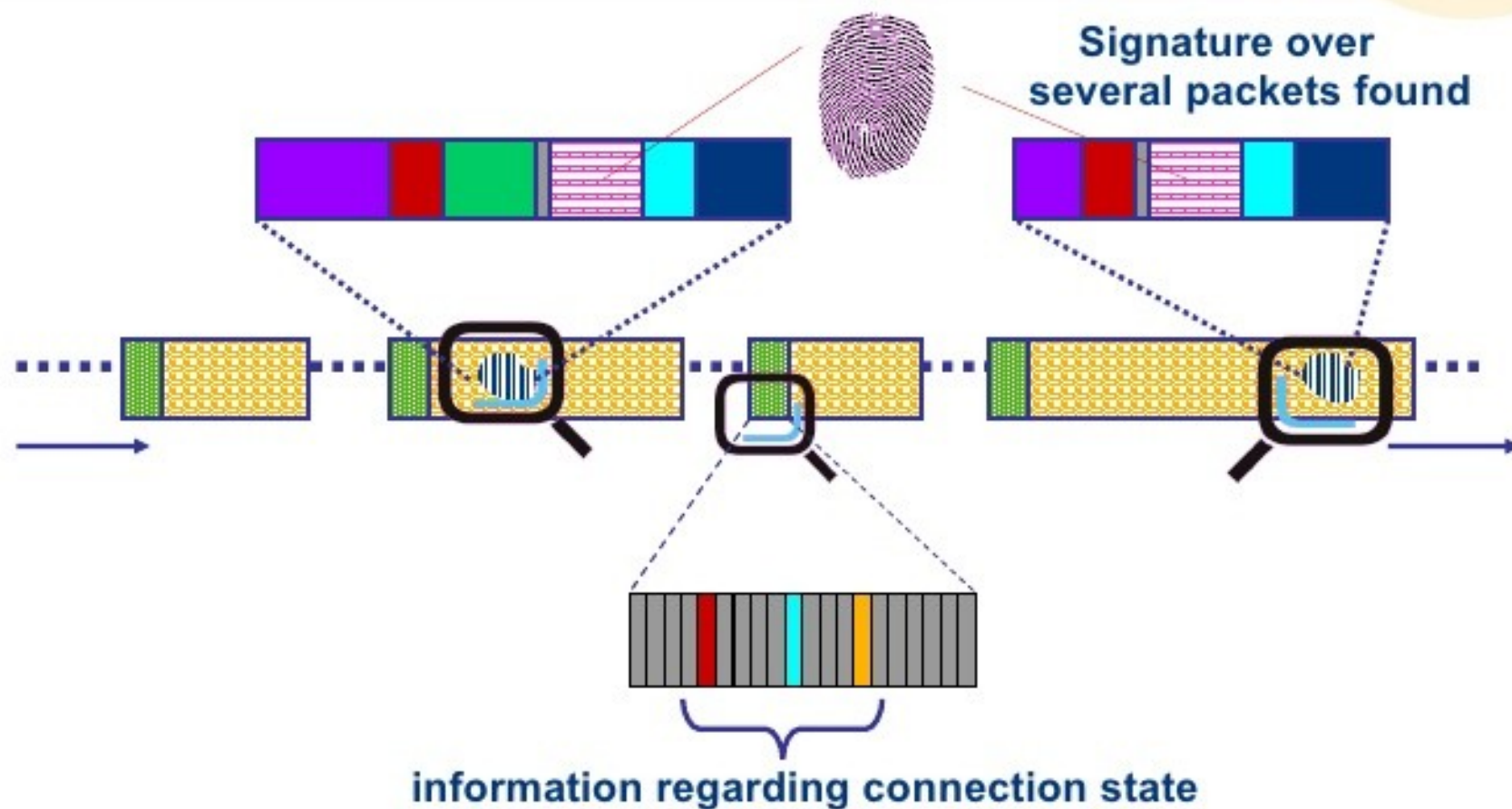
- Allow only requested TCP connections:



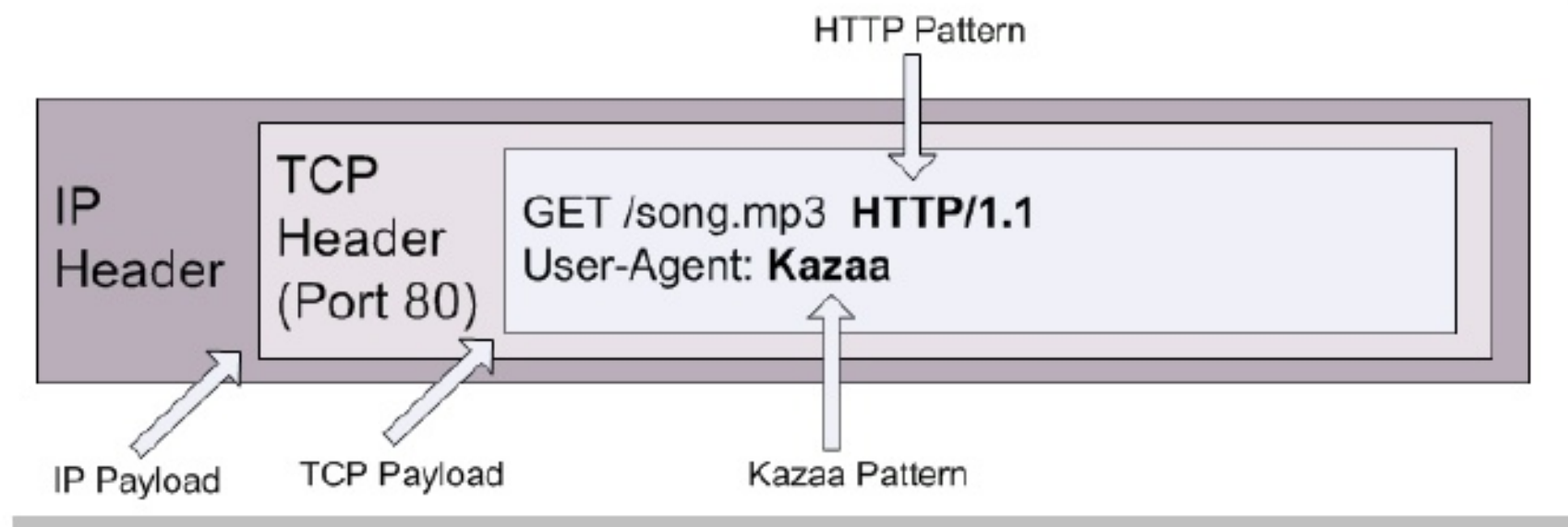
Firewall - Stateful

- Quando é feita uma análise detalhada dos pacotes (conteúdo), opera-se no modo **deep packet inspection**.
- Pode ser utilizado como ferramenta de detecção de intrusões.

Deep Packet Inspection



String Match Example



Firewalk

© February 18, 2014  Information Gathering

Firewalk Package Description

Firewalk is an active reconnaissance network security tool that attempts to determine what layer 4 protocols a given IP forwarding device will pass. Firewalk works by sending out TCP or UDP packets with a TTL one greater than the targeted gateway. If the gateway allows the traffic, it will forward the packets to the next hop where they will expire and elicit an ICMP_TIME_EXCEEDED message. If the gateway host does not allow the traffic, it will likely drop the packets on the floor and we will see no response.

Continua