Responsabilidade de provedores na conexão à Internet

Notas para discussão

Danton Nunes, Internexo Ltda.
(danton.nunes@inexo.com.br)

Responsabilidade de provedores na conexão à Internet

Notas para discussão

Problema: DDoS com spoofing e amplificação.

Diversos atores sob diferentes autoridades:

- **spam e outros mecanismos de injeção de software clandestino**
- **botnets e motherships**
- **spoofing**
- **exploração de serviços abertos (especialmente DNS recursivo)**
- **reação ao ataque: difícil, complexa e requer coordenação.**

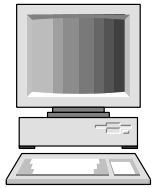
sob a responsabilidade de provedores de serviços!

Mas os provedores seguem as boas práticas para evitar, mitigar e resolver esses problemas?

geralmente **NÃO!**

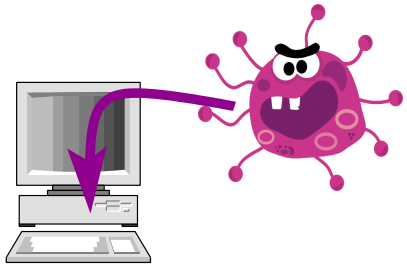
Anatomia do DDoS com amplificação

Anatomia do DDoS com amplificação



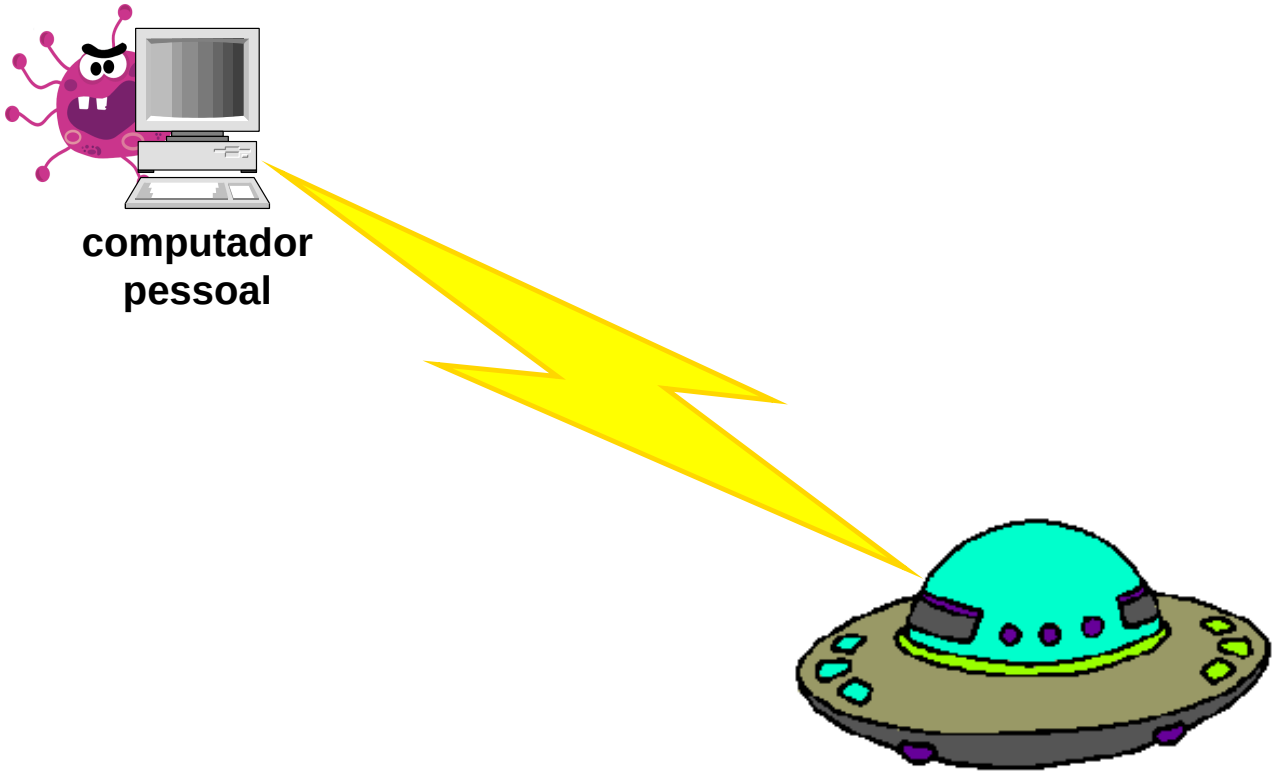
computador pessoal

Anatomia do DDoS com amplificação



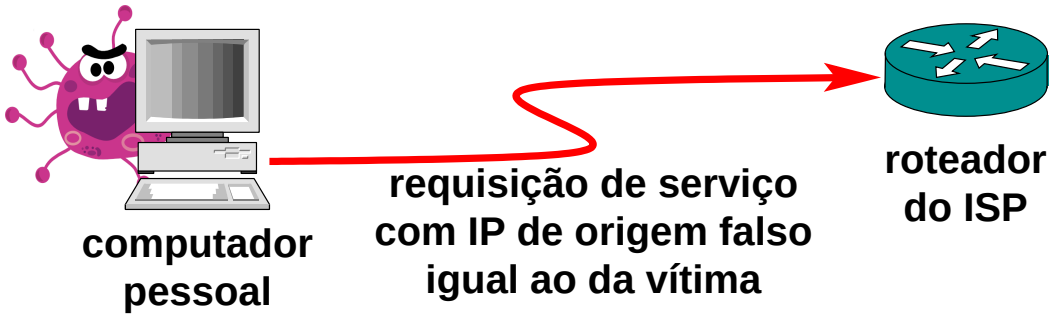
computador
pessoal

Anatomia do DDoS com amplificação

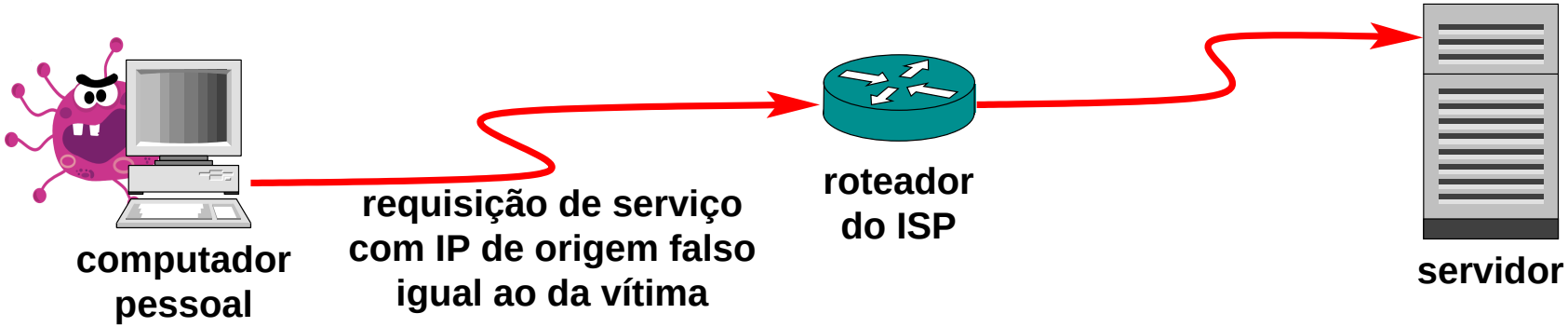


computador pessoal

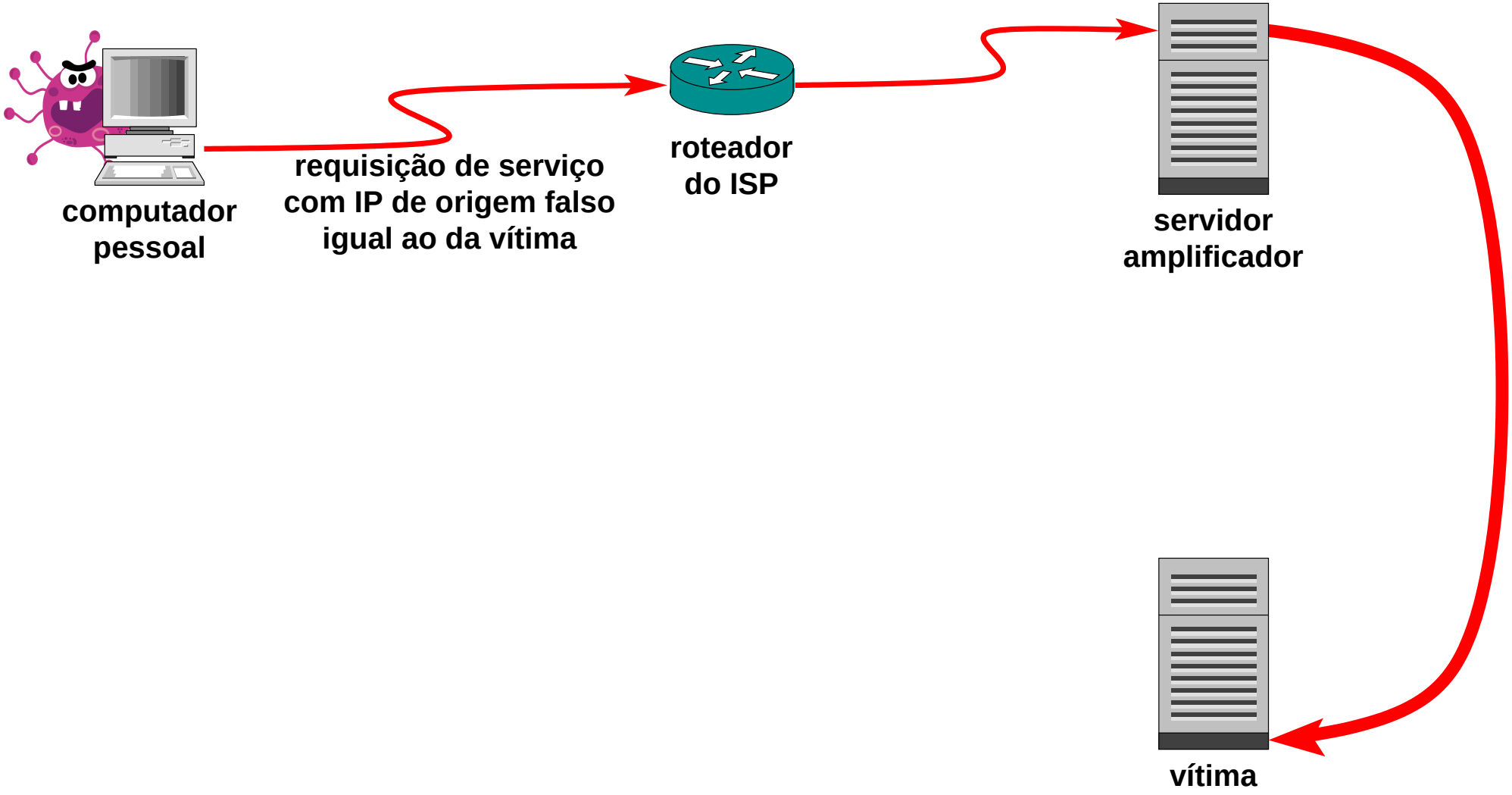
Anatomia do DDoS com amplificação



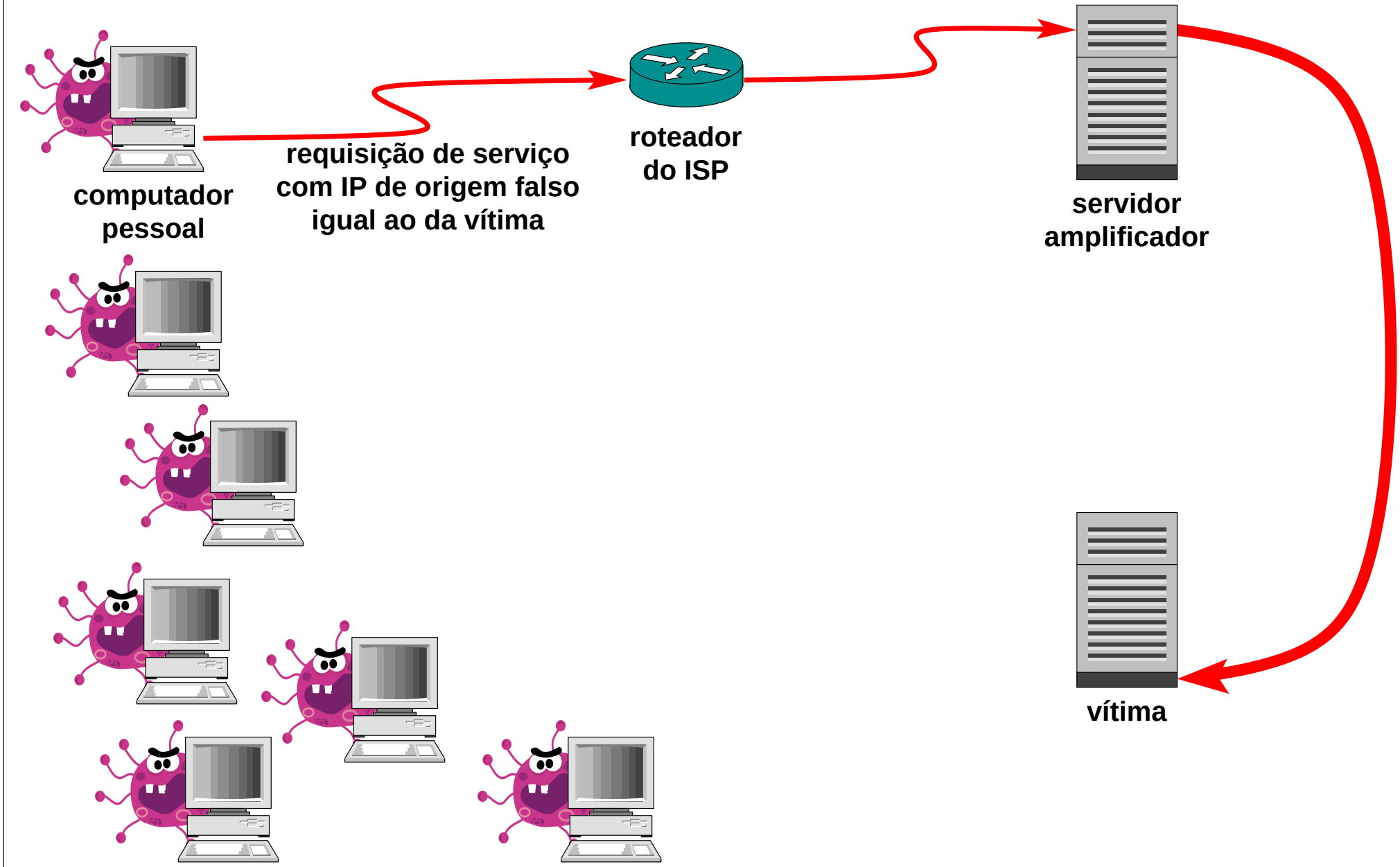
Anatomia do DDoS com amplificação



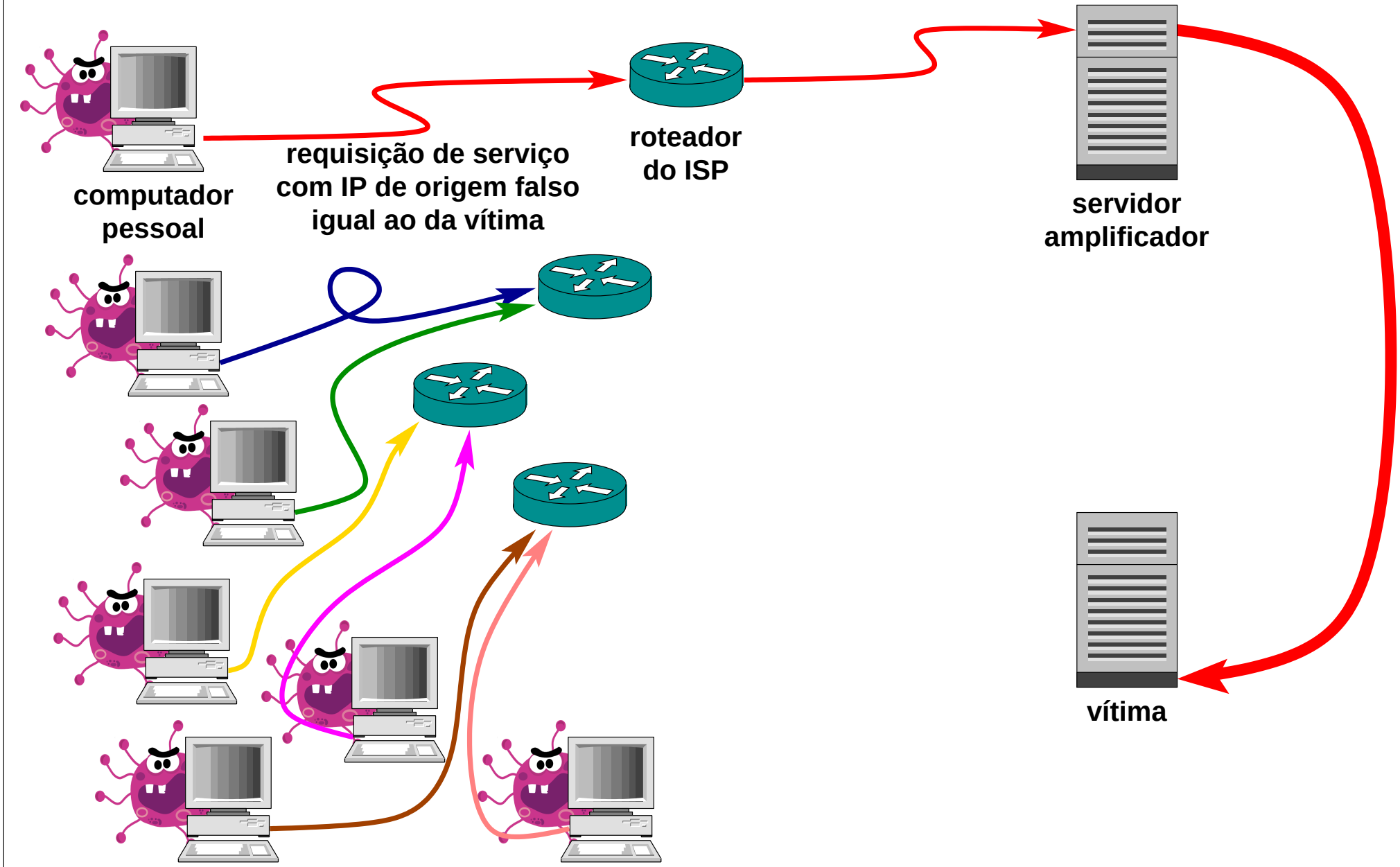
Anatomia do DDoS com amplificação



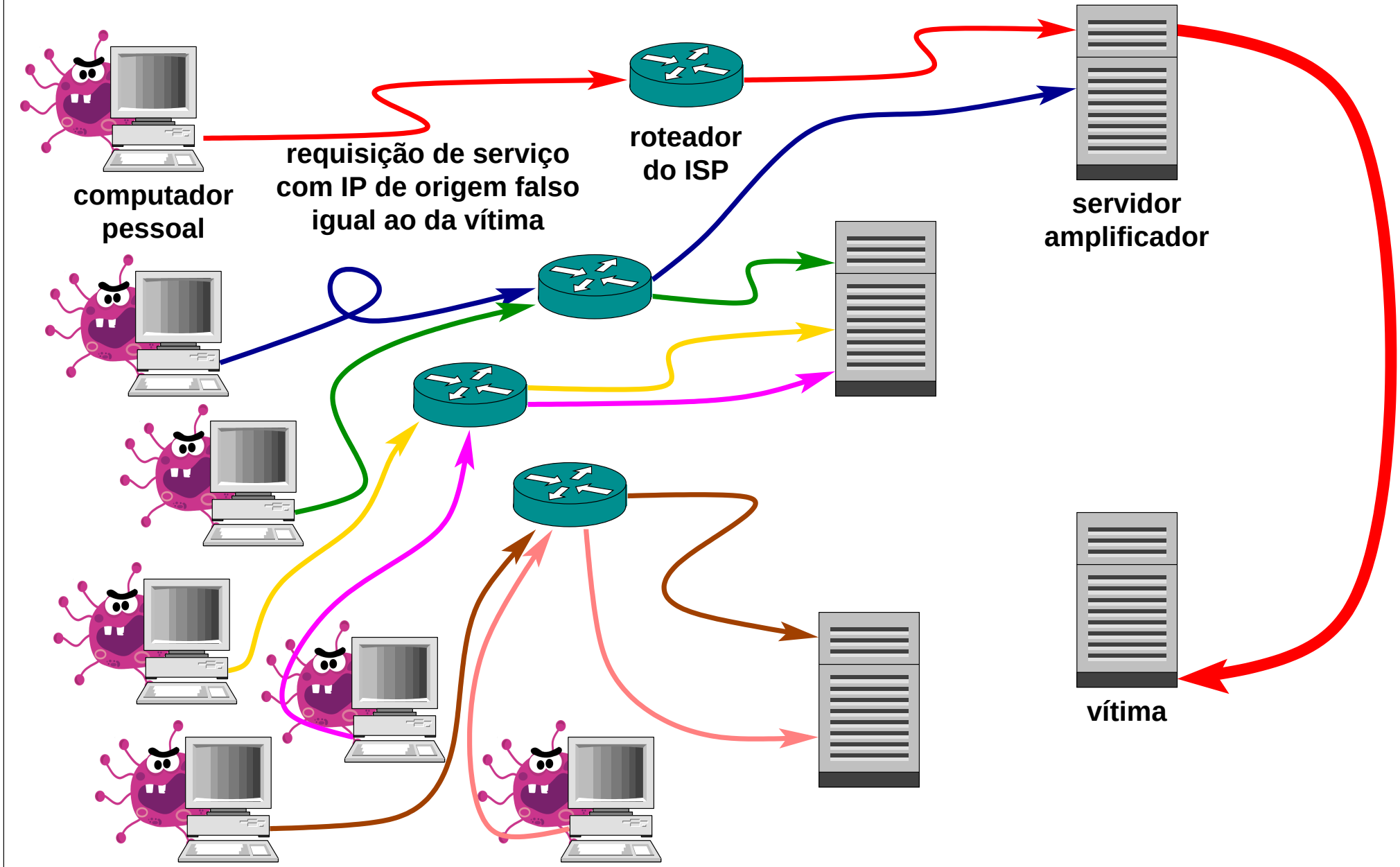
Anatomia do DDoS com amplificação



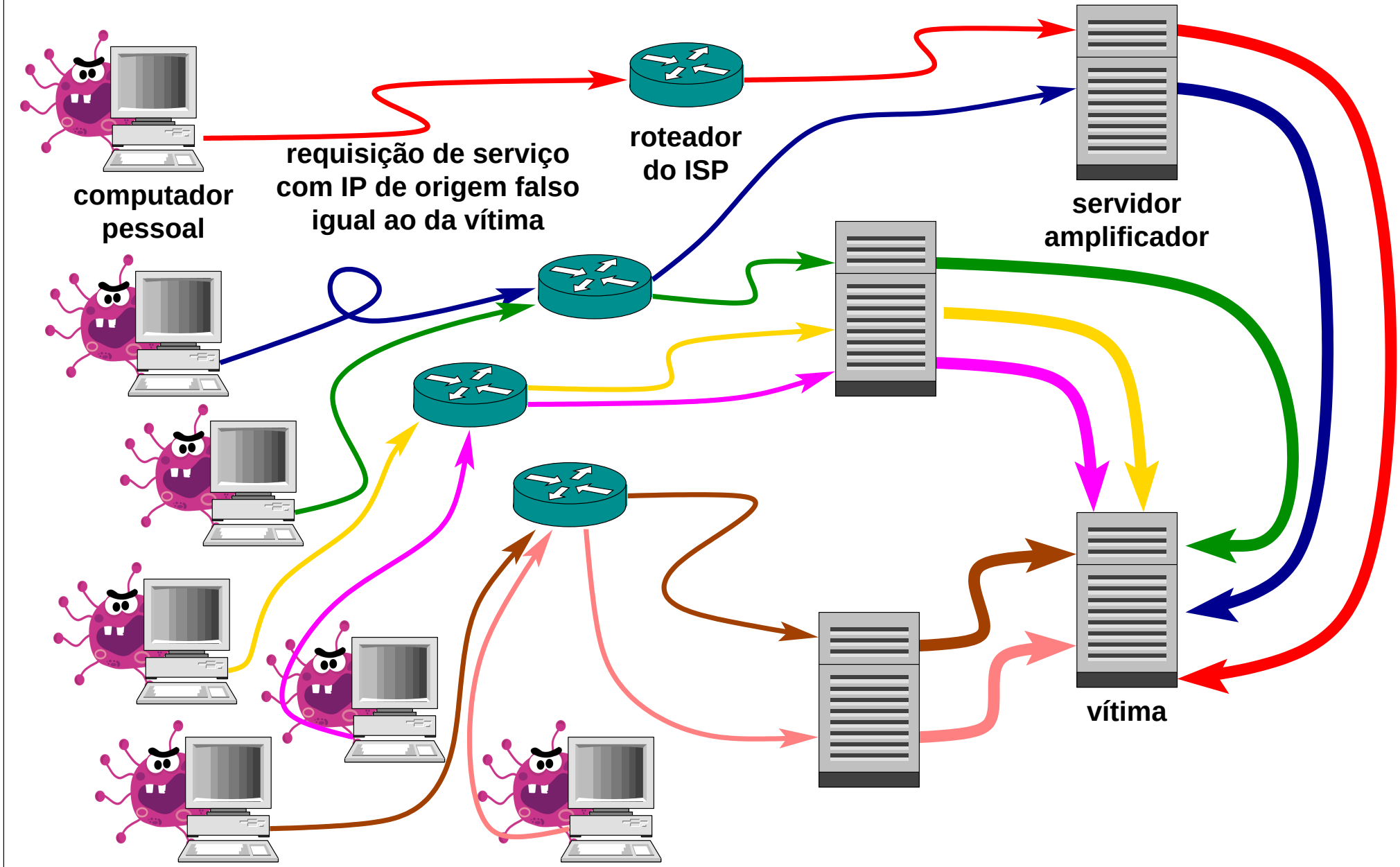
Anatomia do DDoS com amplificação



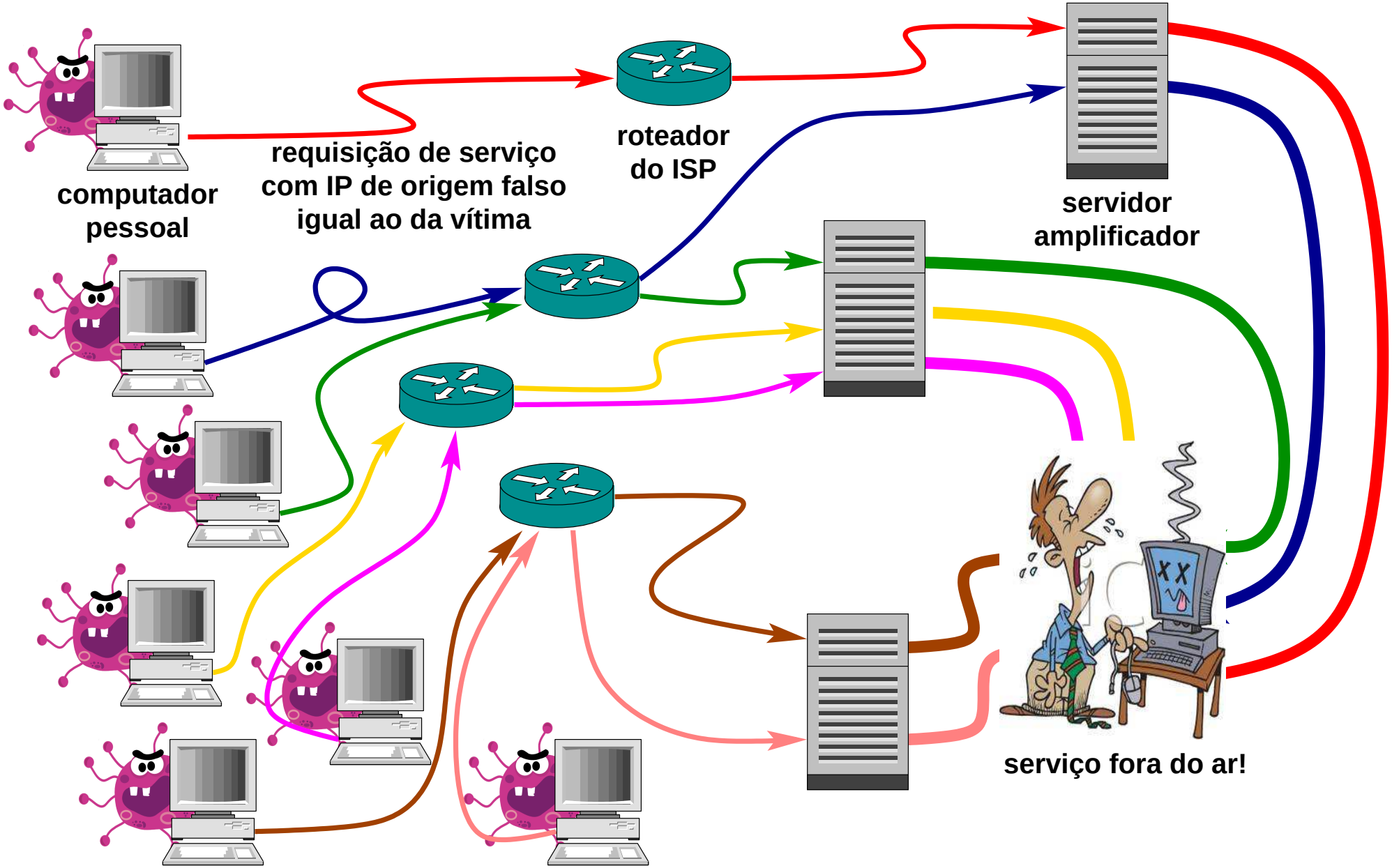
Anatomia do DDoS com amplificação



Anatomia do DDoS com amplificação

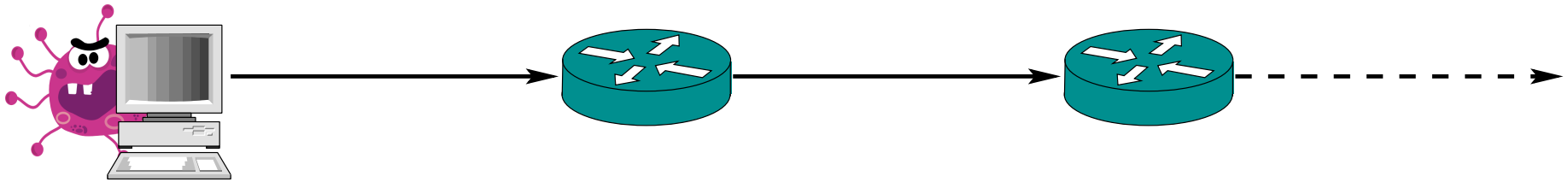


Anatomia do DDoS com amplificação



É aqui que entra a RFC−2827, ou BCP−38

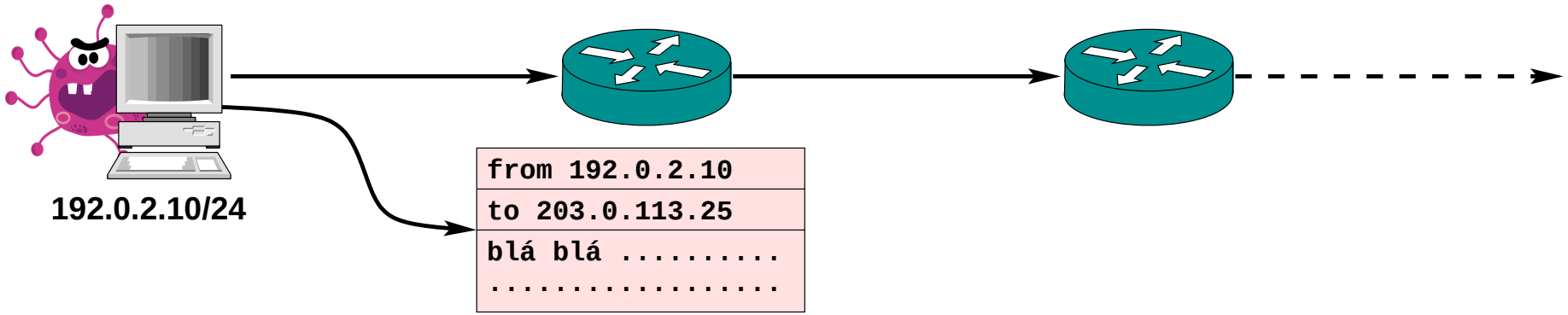
Filtragem de INGRESSO (no roteador)



192.0.2.10/24

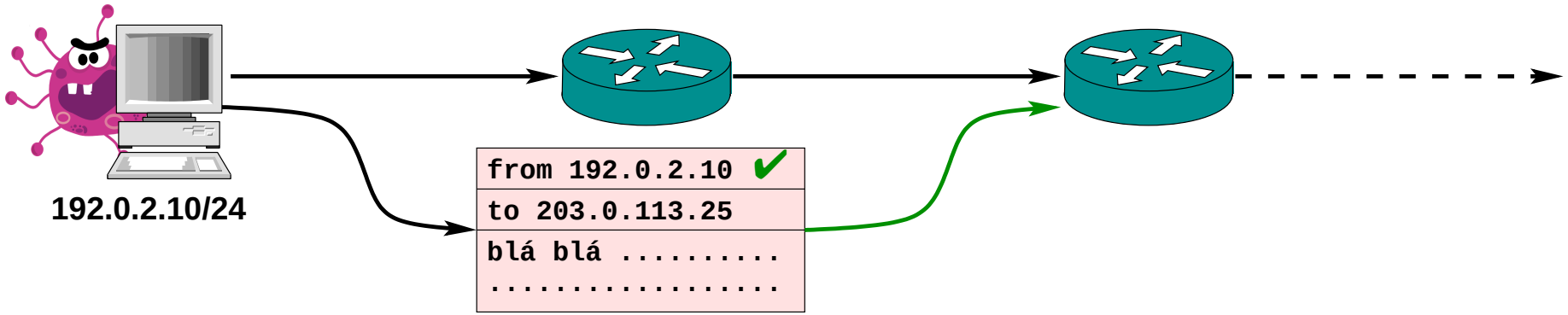
É aqui que entra a RFC−2827, ou BCP−38

Filtragem de INGRESSO (no roteador)



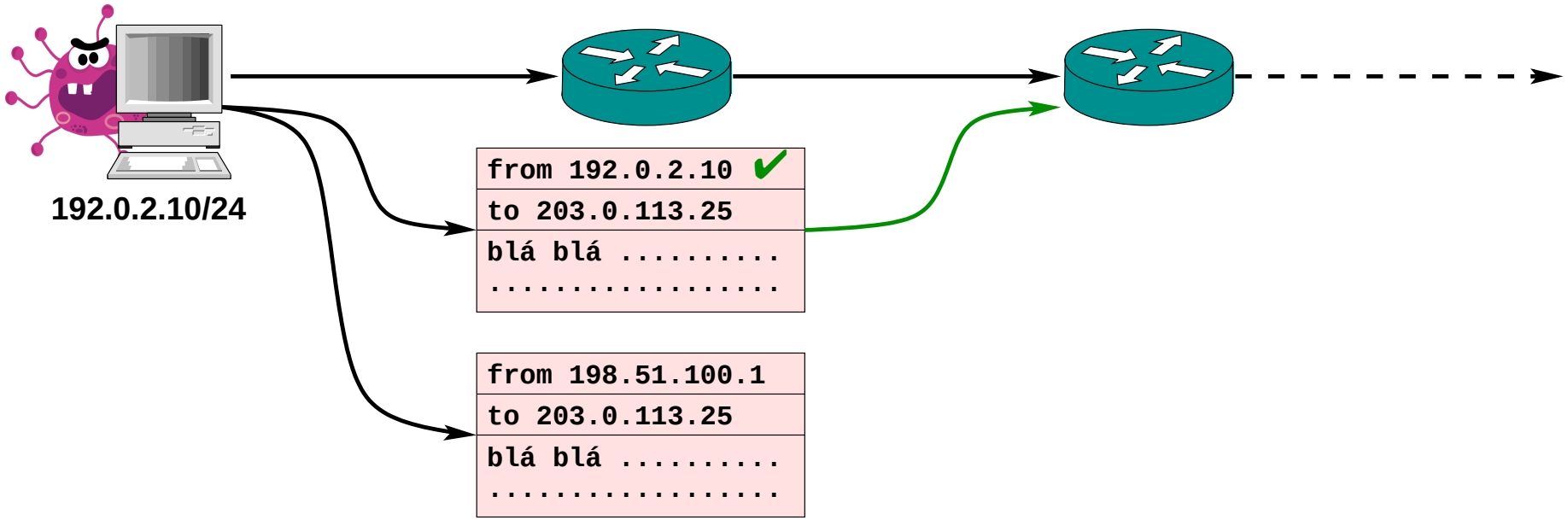
É aqui que entra a RFC−2827, ou BCP−38

Filtragem de INGRESSO (no roteador)



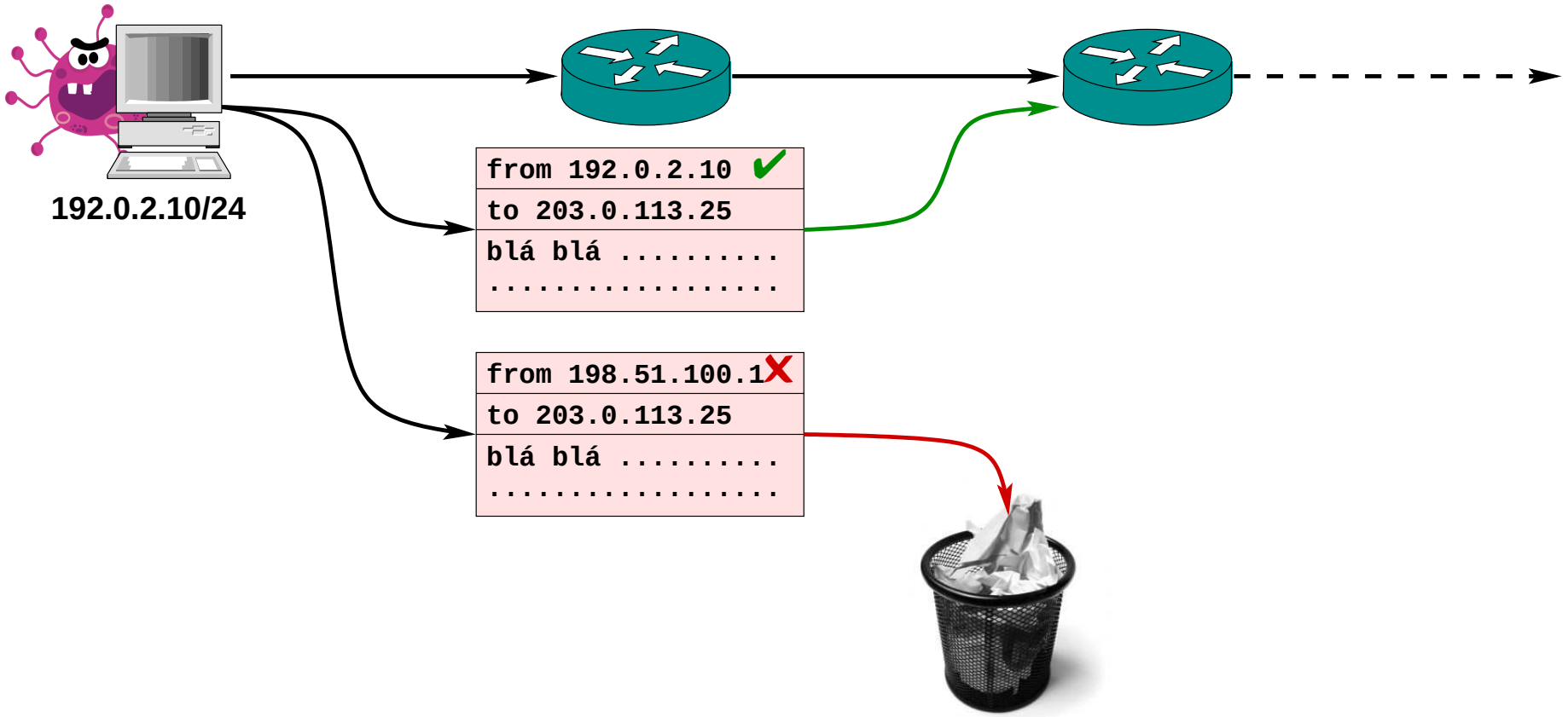
É aqui que entra a RFC−2827, ou BCP−38

Filtragem de INGRESSO (no roteador)



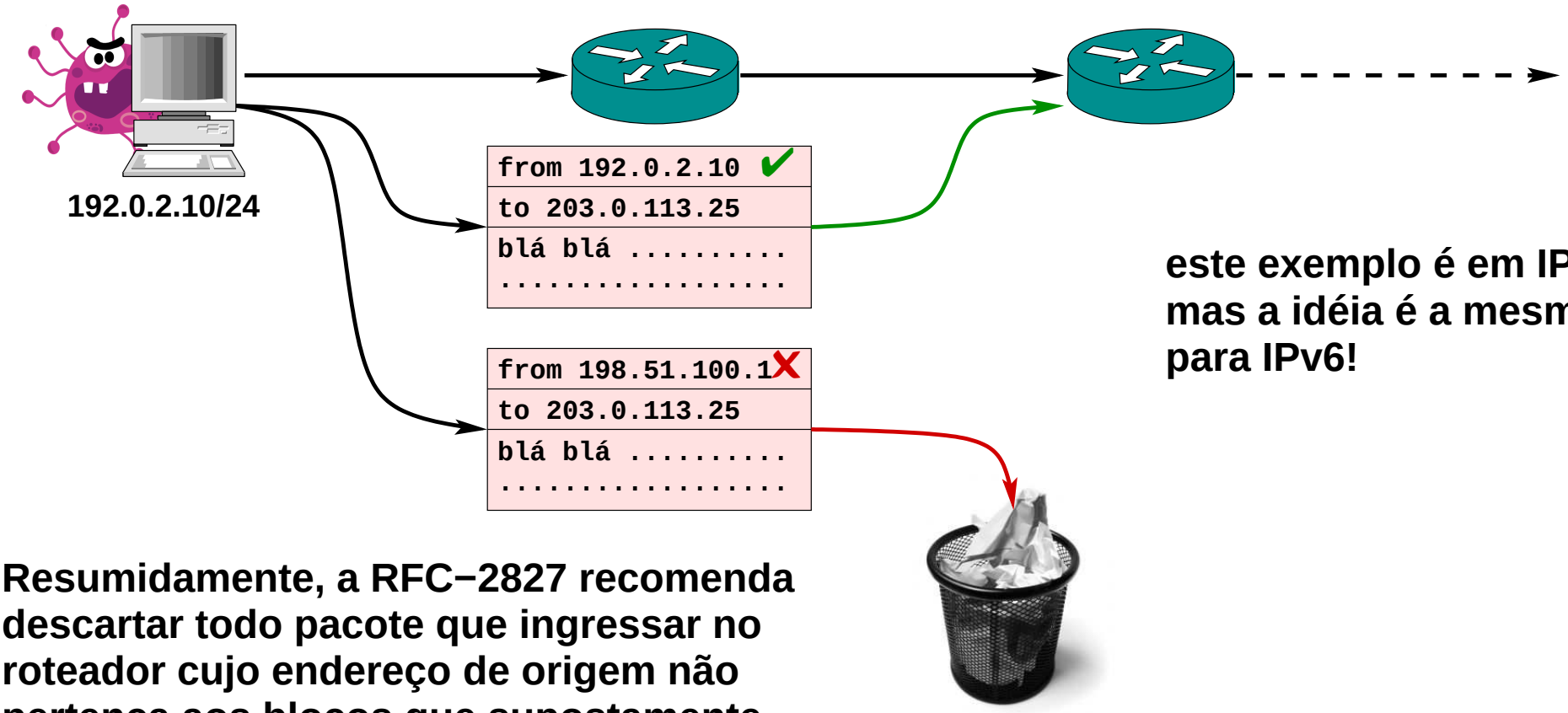
É aqui que entra a RFC−2827, ou BCP−38

Filtragem de INGRESSO (no roteador)



É aqui que entra a RFC−2827, ou BCP−38

Filtragem de INGRESSO (no roteador)



este exemplo é em IPv4, mas a idéia é a mesma para IPv6!

Resumidamente, a RFC−2827 recomenda descartar todo pacote que ingressar no roteador cujo endereço de origem não pertença aos blocos que supostamente estão naquela interface.

É a mais efetiva medida anti−spoofing.

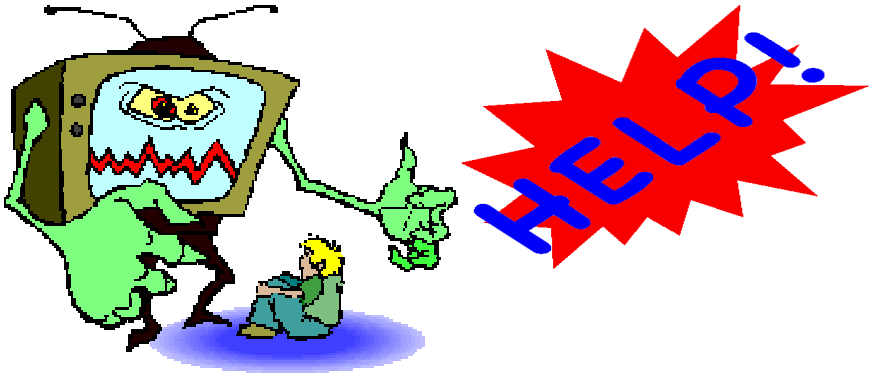
É tão mais efetiva quanto mais perto do usuário final ela for aplicada.

Combinando com LOGs permite identificar qual a maquina que está abrigando o bot.

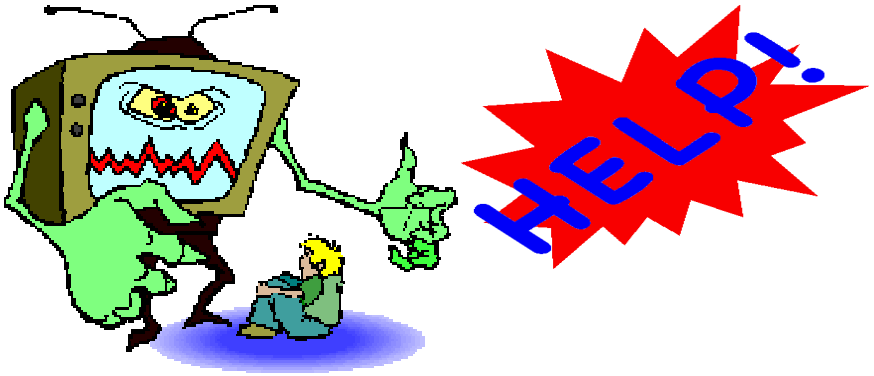
```
#!/bin/bash
#
#       produz regras de ingresso e egresso a partir da tabela de rotas
#
# termina se a interface tem rota default.
[ "$(ip route show dev $1 exact 0.0.0.0/0 table ${2:-main})" ] && {
        echo "$1 has a default route. No ingress/egress filters." >/dev/stderr
        exit 1
}

# cria duas cadeias, uma para cada direção.
ing=ingress-$1
egr=egress-$1
iptables -N $ing
iptables -N $egr

# para cada destino na tabela de rotas da interface cria duas regras
ip route show dev $1 table ${2:-main} | while read prefix garbage
do
        iptables -t filter -A $ing -s $prefix -j RETURN    # ingresso
        iptables -t filter -A $egr -s $prefix -j DROP      # egresso
done

# acrescenta os comportamentos padrão
iptables -t filter -A $ing -j DROP
iptables -t filter -A $egr -j RETURN

# pendura essas cadeias em FORWARD
iptables -t filter -A FORWARD -i $1 -j $ing
iptables -t filter -A FORWARD -o $1 -j $egr
```

E quando o caldo entorna?...

E quando o caldo entorna?...

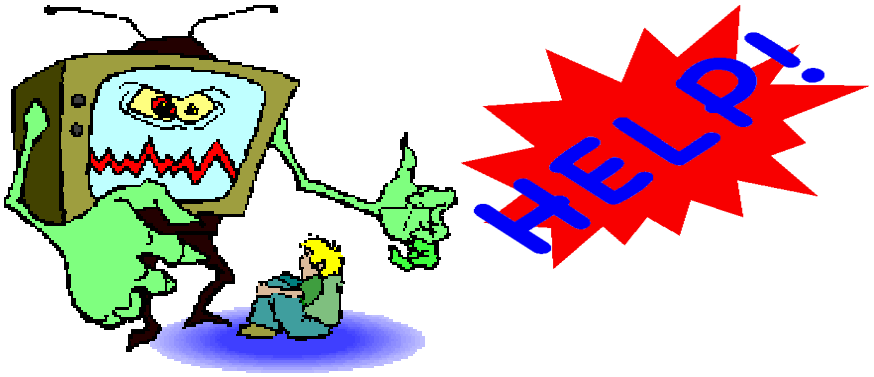


E quando o caldo entorna?...



Você liga para o INOC-DBA

E quando o caldo entorna?...



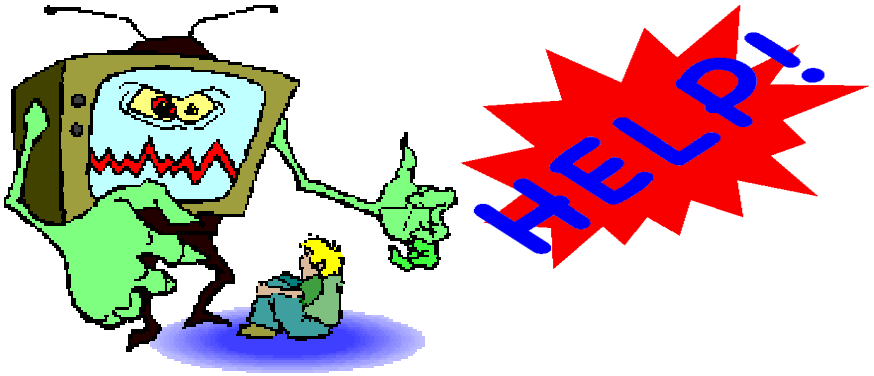
Você liga para o INOC-DBA

Vou mandar um email para abuse@example.net:

```
mail from: <needing@urgent.help.now>
250 2.1.0 <needing@urgent.help.now>... Sender ok
rcpt to: <abuse@example.net>
553 5.1.8 <abuse@example.net> ... User unknown
```

RFC-2142

E quando o caldo entorna?...



Vou ligar para o INOC-DBA

Vou mandar um email para abuse@example.net:

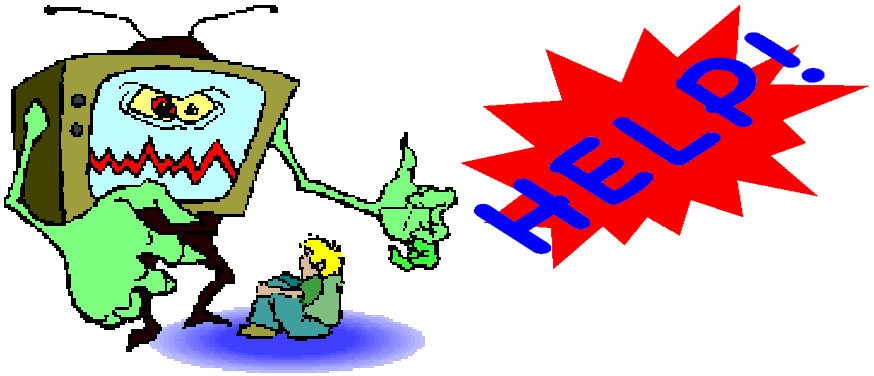
```
mail from: <needing@urgent.help.now>
250 2.1.0 <needing@urgent.help.now>... Sender ok
rcpt to: <abuse@example.net>
553 5.1.8 <abuse@example.net> ... User unknown
```

RFC-2142

Vou procurar os endereços de contato no whois:

```
abuse-c:      MANE
...
nic-hdl-br:   MANE
person:       Ze Mane da Silva
e-mail:       no.longer.works.here@example.net
```

E quando o caldo entorna?...



Vou ligar para o INOC-DBA

Vou mandar um email para abuse@example.net:

```
mail from: <needing@urgent.help.now>
250 2.1.0 <needing@urgent.help.now>... Sender ok
rcpt to: <abuse@example.net>
553 5.1.8 <abuse@example.net> ... User unknown
```

RFC-2142

Vou procurar os endereços de contato no whois:

```
abuse-c:      MANE
...
nic-hdl-br:   MANE
person:       Ze Mane da Silva
e-mail:       no.longer.works.here@example.net
```

.... precisa ter MUITA paciência .....

É aqui que entra a RFC−3031, ou BCP−46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
  1.1 Conventions Used in this Document. 3
2 Communication. 3
  2.1 Contact Information. 3
  2.2 Information Sharing. 4
  2.3 Secure Channels. 4
  2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
  2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
  3.1 Announcement of Policy 6
  3.2 Sanctions. 6
  3.3 Data Protection. 6
4 Network Infrastructure 6
  4.1 Registry Data Maintenance. 6
  4.2 Routing Infrastructure 7
  4.3 Ingress Filtering on Source Address. 7
  4.4 Egress Filtering on Source Address 8
  4.5 Route Filtering. 8
  4.6 Directed Broadcast 8
5 Systems Infrastructure 9
  5.1 System Management. 9
  5.2 No Systems on Transit Networks 9
  5.3 Open Mail Relay. 9
  5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
  1.1 Conventions Used in this Document. 3
2 Communication. 3
  2.1 Contact Information. 3
  2.2 Information Sharing. 4
  2.3 Secure Channels. 4
  2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
  2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
  3.1 Announcement of Policy 6
  3.2 Sanctions. 6
  3.3 Data Protection. 6
4 Network Infrastructure 6
  4.1 Registry Data Maintenance. 6
  4.2 Routing Infrastructure 7
  4.3 Ingress Filtering on Source Address. 7
  4.4 Egress Filtering on Source Address 8
  4.5 Route Filtering. 8
  4.6 Directed Broadcast 8
5 Systems Infrastructure 9
  5.1 System Management. 9
  5.2 No Systems on Transit Networks 9
  5.3 Open Mail Relay. 9
  5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

contatos e troca de informações.

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
1.1 Conventions Used in this Document. 3
2 Communication. 3
2.1 Contact Information. 3
2.2 Information Sharing. 4
2.3 Secure Channels. 4
2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
3.1 Announcement of Policy 6
3.2 Sanctions. 6
3.3 Data Protection. 6
4 Network Infrastructure 6
4.1 Registry Data Maintenance. 6
4.2 Routing Infrastructure 7
4.3 Ingress Filtering on Source Address. 7
4.4 Egress Filtering on Source Address 8
4.5 Route Filtering. 8
4.6 Directed Broadcast 8
5 Systems Infrastructure 9
5.1 System Management. 9
5.2 No Systems on Transit Networks 9
5.3 Open Mail Relay. 9
5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

contatos e troca de informações.

política de uso e relações com clientes

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
1.1 Conventions Used in this Document. 3
2 Communication. 3
2.1 Contact Information. 3
2.2 Information Sharing. 4
2.3 Secure Channels. 4
2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
3.1 Announcement of Policy 6
3.2 Sanctions. 6
3.3 Data Protection. 6
4 Network Infrastructure 6
4.1 Registry Data Maintenance. 6
4.2 Routing Infrastructure 7
4.3 Ingress Filtering on Source Address. 7
4.4 Egress Filtering on Source Address 8
4.5 Route Filtering. 8
4.6 Directed Broadcast 8
5 Systems Infrastructure 9
5.1 System Management. 9
5.2 No Systems on Transit Networks 9
5.3 Open Mail Relay. 9
5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

contatos e troca de informações.

política de uso e relações com clientes

infraestrutura de rede, filtragem de pacotes, e afins.

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
1.1 Conventions Used in this Document. 3
2 Communication. 3
2.1 Contact Information. 3
2.2 Information Sharing. 4
2.3 Secure Channels. 4
2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
3.1 Announcement of Policy 6
3.2 Sanctions. 6
3.3 Data Protection. 6
4 Network Infrastructure 6
4.1 Registry Data Maintenance. 6
4.2 Routing Infrastructure 7
4.3 Ingress Filtering on Source Address. 7
4.4 Egress Filtering on Source Address 8
4.5 Route Filtering. 8
4.6 Directed Broadcast 8
5 Systems Infrastructure 9
5.1 System Management. 9
5.2 No Systems on Transit Networks 9
5.3 Open Mail Relay. 9
5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

contatos e troca de informações.

política de uso e relações com clientes

infraestrutura de rede, filtragem de pacotes, e afins.

gerenciamento de sistemas e aplicações.

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
1.1 Conventions Used in this Document. 3
2 Communication. 3
2.1 Contact Information. 3
2.2 Information Sharing. 4
2.3 Secure Channels. 4
2.4 Notification of Vulnerabilities and Reporting Incidents. . . 4
2.5 ISPs and Computer Security Incident Response Teams (CSIRTs). 5
3 Appropriate Use Policy 5
3.1 Announcement of Policy 6
3.2 Sanctions. 6
3.3 Data Protection. 6
4 Network Infrastructure 6
4.1 Registry Data Maintenance. 6
4.2 Routing Infrastructure 7
4.3 Ingress Filtering on Source Address. 7
4.4 Egress Filtering on Source Address 8
4.5 Route Filtering. 8
4.6 Directed Broadcast 8
5 Systems Infrastructure 9
5.1 System Management. 9
5.2 No Systems on Transit Networks 9
5.3 Open Mail Relay. 9
5.4 Message Submission 9
6 References 10
7 Acknowledgements 12
8 Security Considerations. 12
9 Author’s Address 12
10 Full Copyright Statement. 13

contatos e troca de informações.

política de uso e relações com clientes

infraestrutura de rede, filtragem de pacotes, e afins.

gerenciamento de sistemas e aplicações.

"burocracia"

É aqui que entra a RFC–3031, ou BCP–46

Recommended Internet Service Provider Security Services and Procedures

13 páginas da mais pura expressão do bom senso!

1 Introduction 2
  1.1 Conventions Used in this Document. 3
2 Communication. . . . . .
  2.1 Contact Information. . . . . .
  2.2 Information Sharing. . . . . .
  2.3 Secure Channels. . . . . .
  2.4 Notification of Vulnerabilities and Reporting Incidents.
  2.5 ISPs and Computer Security Incident Response Teams (CSIRTs
3 Appropriate Use Policy . . . . . .
  3.1 Announcement of Policy . . . . . .
  3.2 Sanctions. . . . . .
  3.3 Data Protection. . . . . .
4 Network Infrastructure . . . . . .
  4.1 Registry Data Maintenance. . . . . .
  4.2 Routing Infrastructure . . . . . .
  4.3 Ingress Filtering on Source Address. . . . . .
  4.4 Egress Filtering on Source Address . . . . . .
  4.5 Route Filtering. . . . . .
  4.6 Directed Broadcast . . . . . .
5 Systems Infrastructure . . . . . .
  5.1 System Management. . . . . .
  5.2 No Systems on Transit Networks . . . . . .
  5.3 Open Mail Relay. . . . . .
  5.4 Message Submission . . . . . .
6 References . . . . . .
7 Acknowledgements . . . . . .
8 Security Considerations. . . . . .
9 Author's Address . . . . . .
10 Full Copyright Statement. . . . . .

Mas a RFC−3031 não é tudo!

Mas a RFC−3031 não é tudo!

Parelhamento (peering):

- bilateral
- multilateral, com servidor de rotas

Mas a RFC−3031 não é tudo!

Parelhamento (peering):

- bilateral
- multilateral, com servidor de rotas

Filtragem de rotas recebidas (marcianos, bogons)

Mas a RFC−3031 não é tudo!

Parelhamento (peering):

- bilateral
- multilateral, com servidor de rotas

Filtragem de rotas recebidas (marcianos, bogons)

Não anunciar besteira!

Mas a RFC−3031 não é tudo!

Parelhamento (peering):

- bilateral
- multilateral, com servidor de rotas

Filtragem de rotas recebidas (marcianos, bogons)

Não anunciar besteira!

Usar adequadamente as comunidades do BGP

Mas a RFC−3031 não é tudo!

Parelhamento (peering):

- bilateral
- multilateral, com servidor de rotas

Filtragem de rotas recebidas (marcianos, bogons)

Não anunciar besteira!

Usar adequadamente as comunidades do BGP

Ideias?

Request For Comments

Read and

For

Comments

Read and Follow Comments

Read and Follow Carefully!