

## DDoS protection measures in the BSD Kernel for modern SMTP gateways

# accf\_smtp, DDoS protection for SMTP

## About the speaker

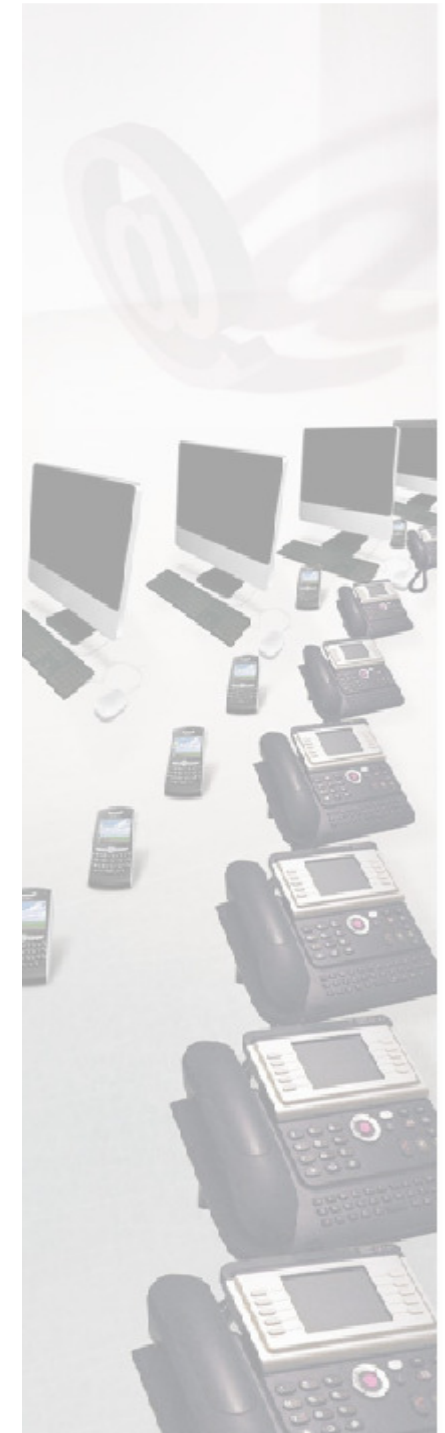
- **About me:**

Martin Blapp, 33 years old  
Currently living in Bubendorf, BL

- **Employment History:**

1998 – 1999 : Solnet GmbH, Zuchwil SO  
1999 – 2008 : ImproWare AG, Pratteln BL  
currently : T-Systems Switzerland, Zollikofen BE

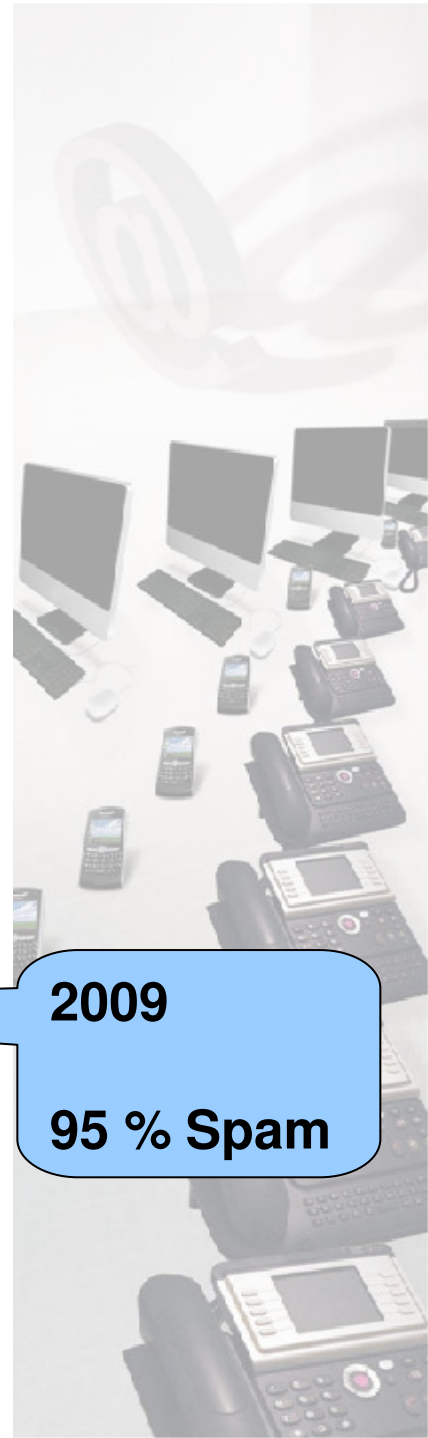
- **E-Mail:** [martin.blapp@t-systems.ch](mailto:martin.blapp@t-systems.ch)  
[mbr@freebsd.org](mailto:mbr@freebsd.org)



# accf\_smtp, DDoS protection for SMTP

## The basic challenge

1999  
10 % Spam



2009  
95 % Spam

# accf\_smtp, DDoS protection for SMTP

## Direct and indirect SMTP attacks: whats the difference ?

### Indirect attacks:

Abuse of ISP infrastructure  
Backscatter traffic from  
„misconfigured“ mailservers

### Solution:

blocking originating IP  
BATV

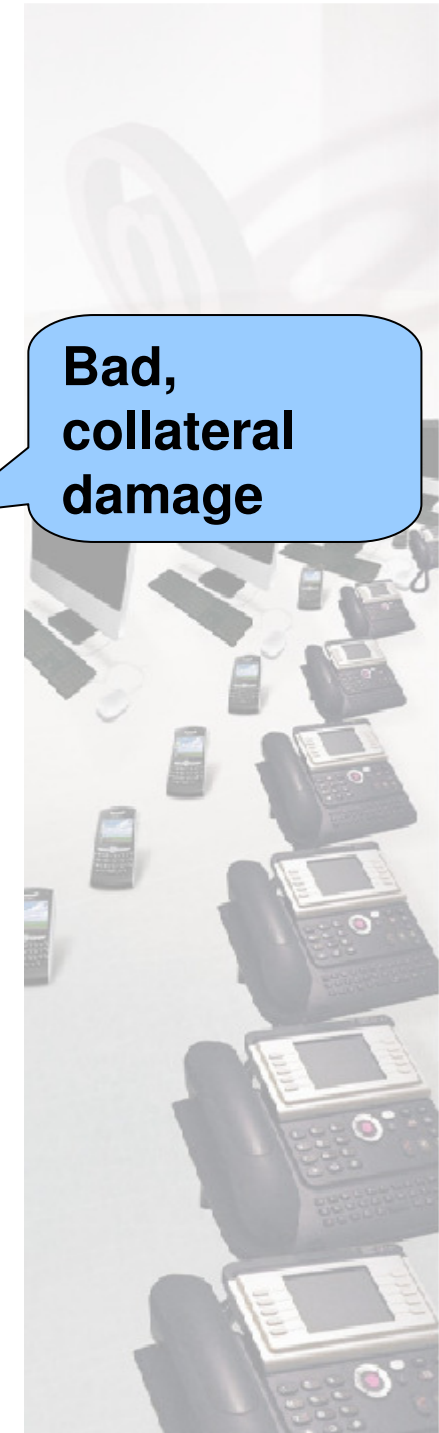
Bad,  
collateral  
damage

### Direct attacks:

Bandwith DoS attacks  
DoS attacks from single IP  
SynFlood attacks  
DDoS attacks from many IPs

### Solution:

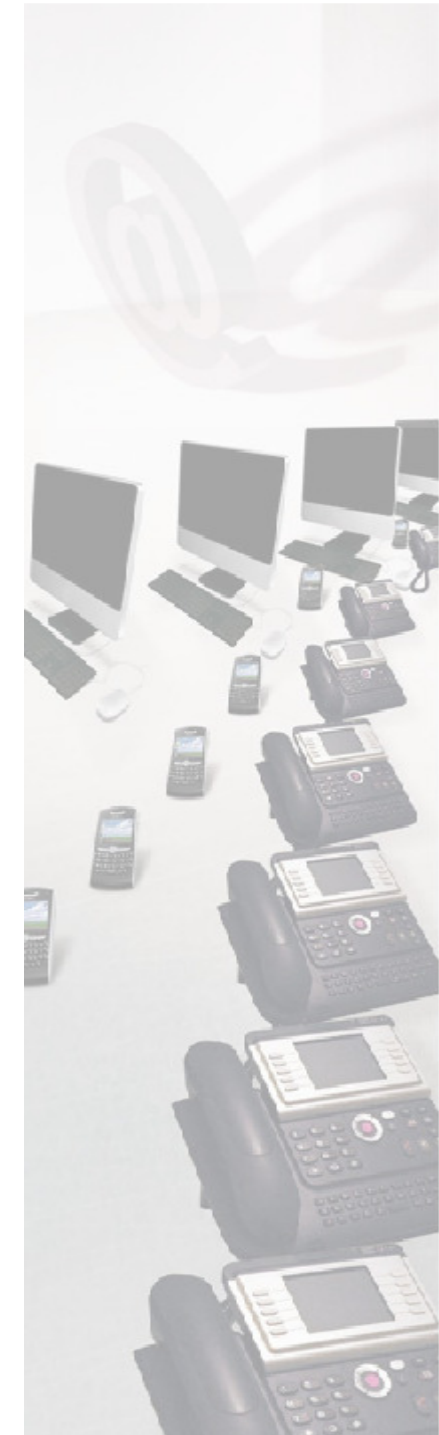
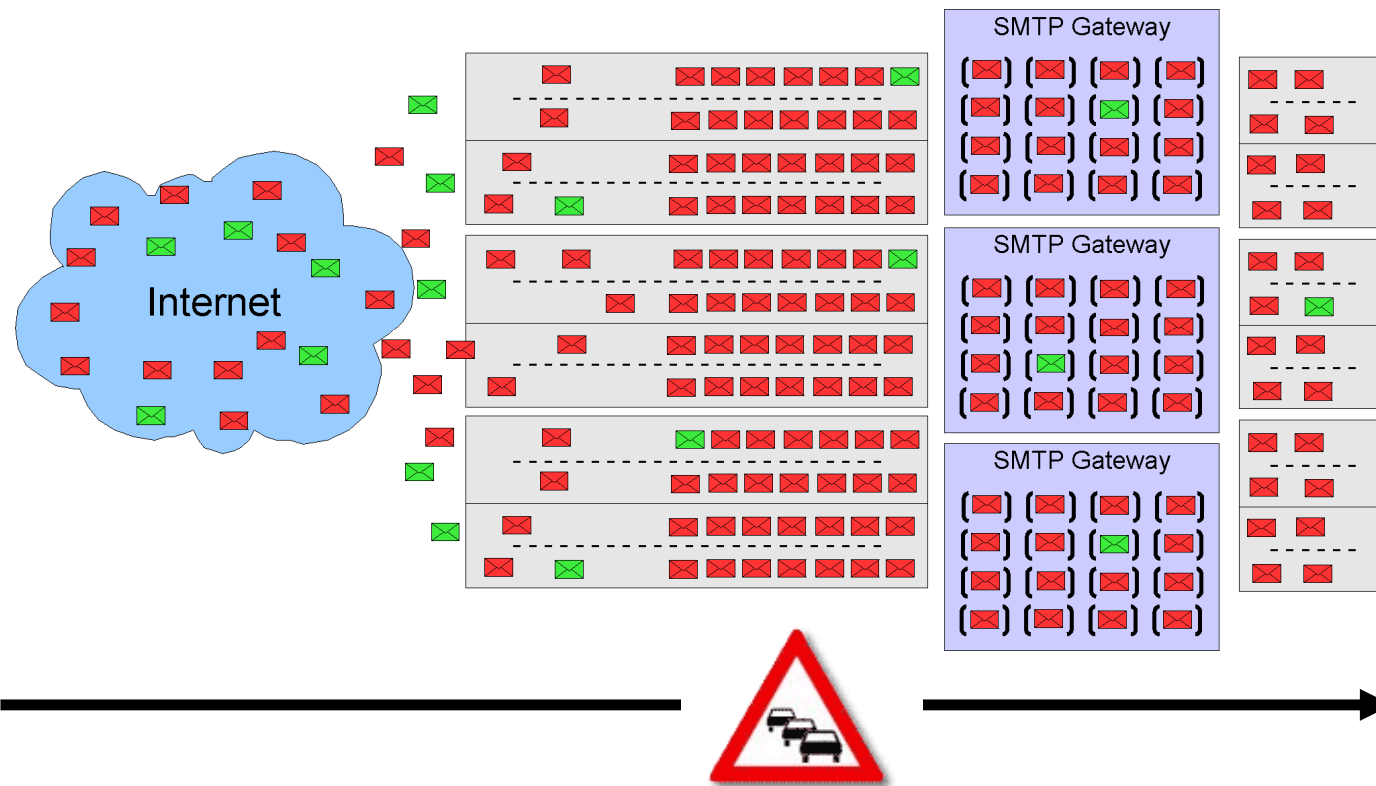
blocking on core router  
blocking originating IP  
syn cookies  
no solution available ?



# accf\_smtp, DDoS protection for SMTP

## The basic challenge

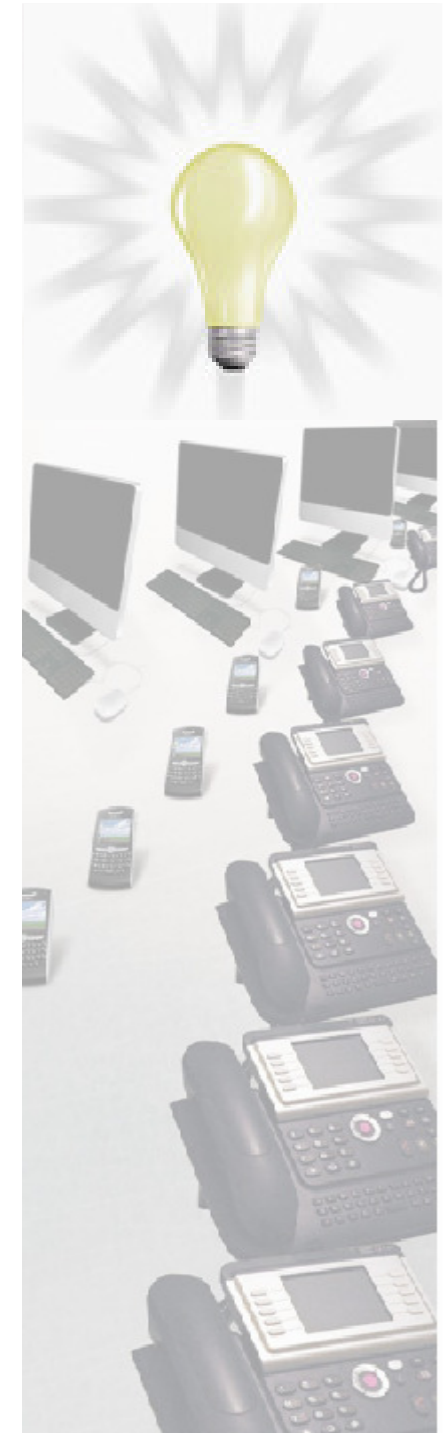
Easy Solution: more hardware ... Really ?



# accf\_smtp, DDoS protection for SMTP

## Kernel filtering advantages:

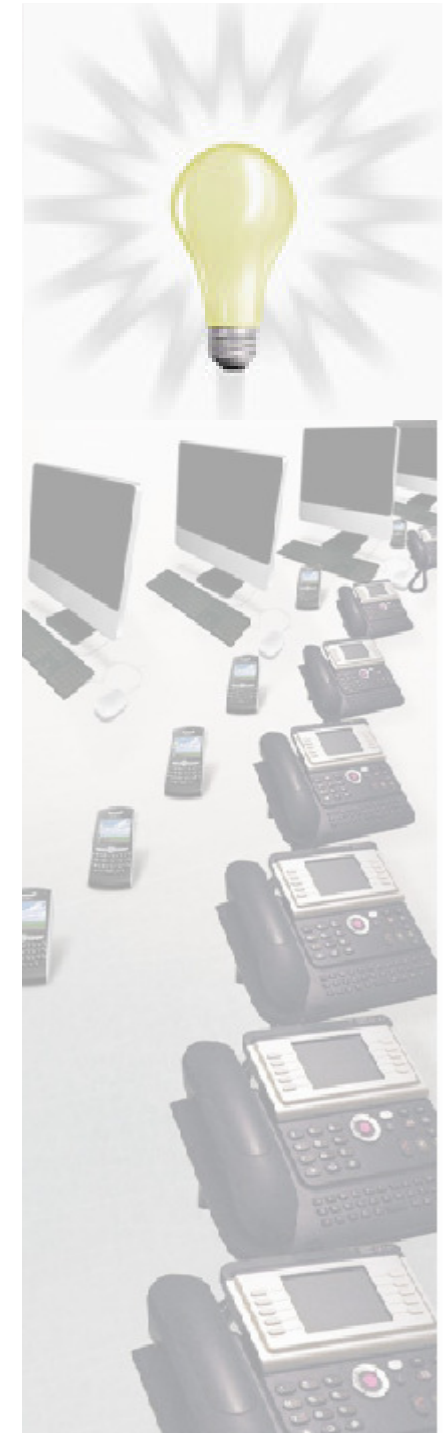
- **Very fast**
- **Very low memory footprint**
- **No context-switches, CPU friendly**
- **No forking, to thread handling needed**
- **Overflow mechanisms easy implementable**



# accf\_smtp, DDoS protection for SMTP

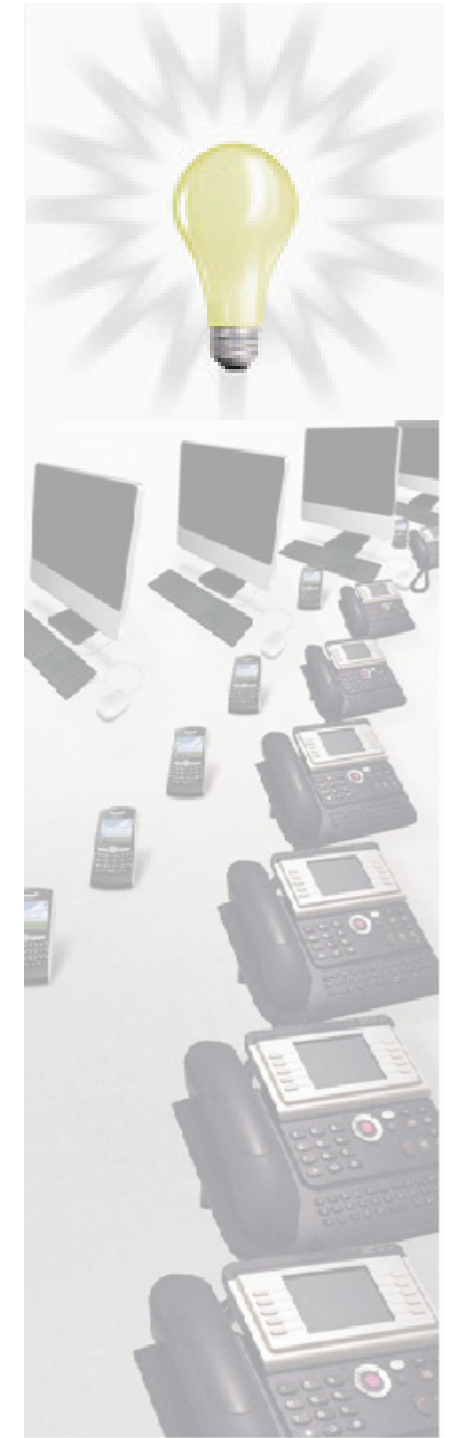
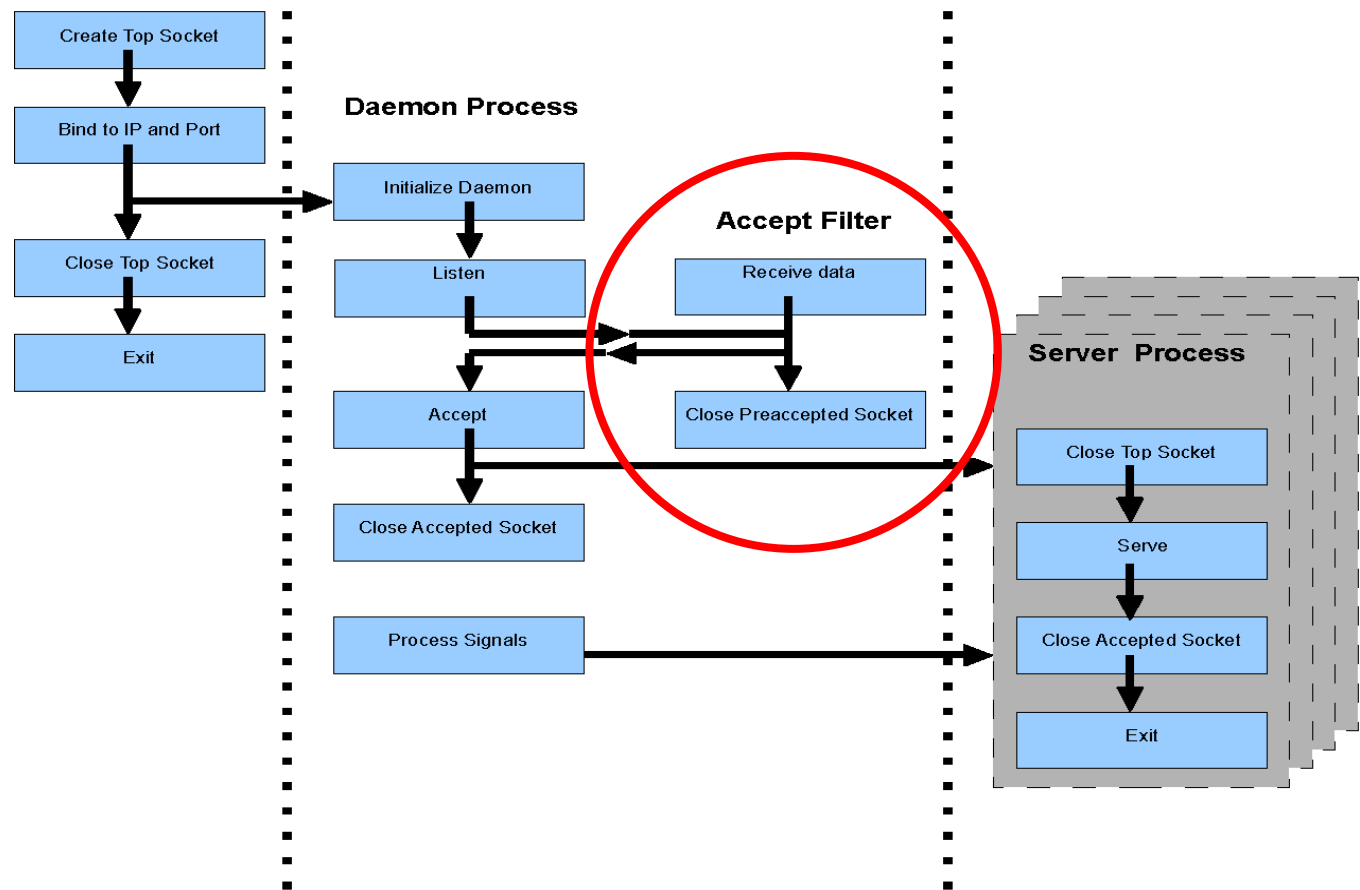
## accf\_smtp – how it works

- Similar to tarpits, but in the OS-kernel
- Offers greetpause functionality in the OS-kernel
- Defers the accept until the first SMTP command is complete
- Kind of SMTP proxy in the OS-kernel
- SMTP firewall for first connection attempts:
  - Validates the length of HELO/EHLO commands
  - Checks for FROM before HELO commands
  - Limits the allowed command set



# accf\_smtp, DDoS protection for SMTP

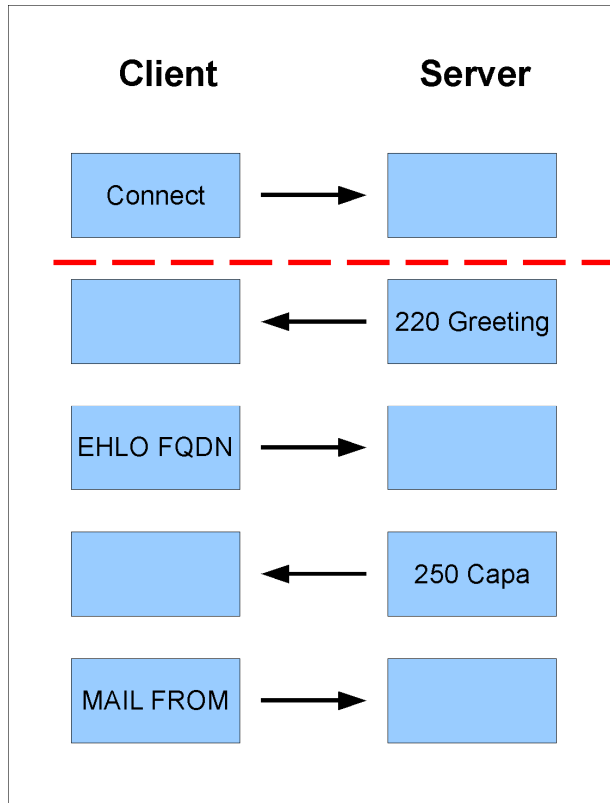
## accf\_smtp - how it works





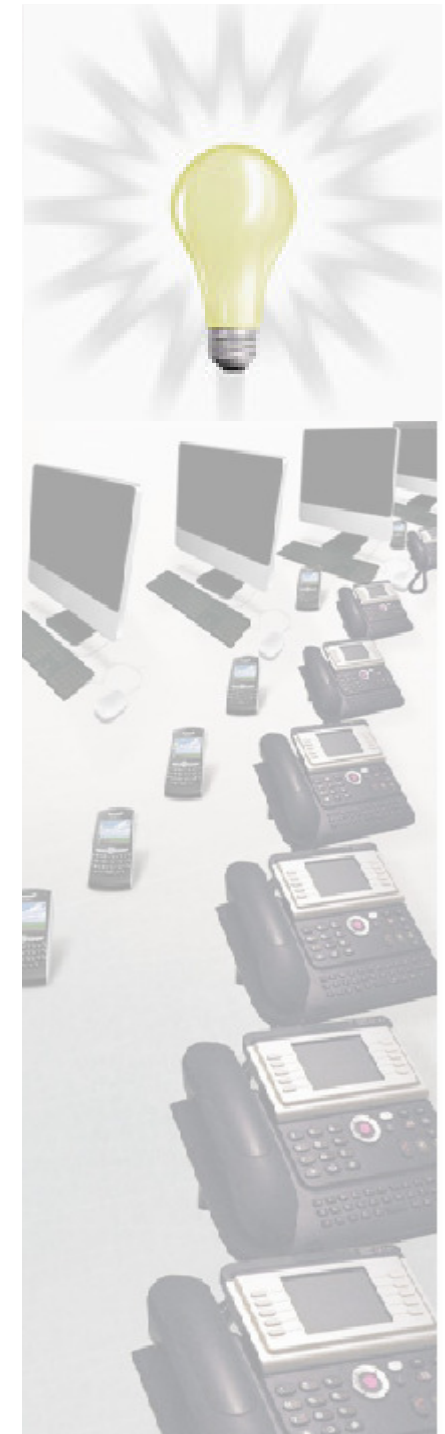
# accf\_smtp, DDoS protection for SMTP

## accf\_smtp - how it works



Greetpause:

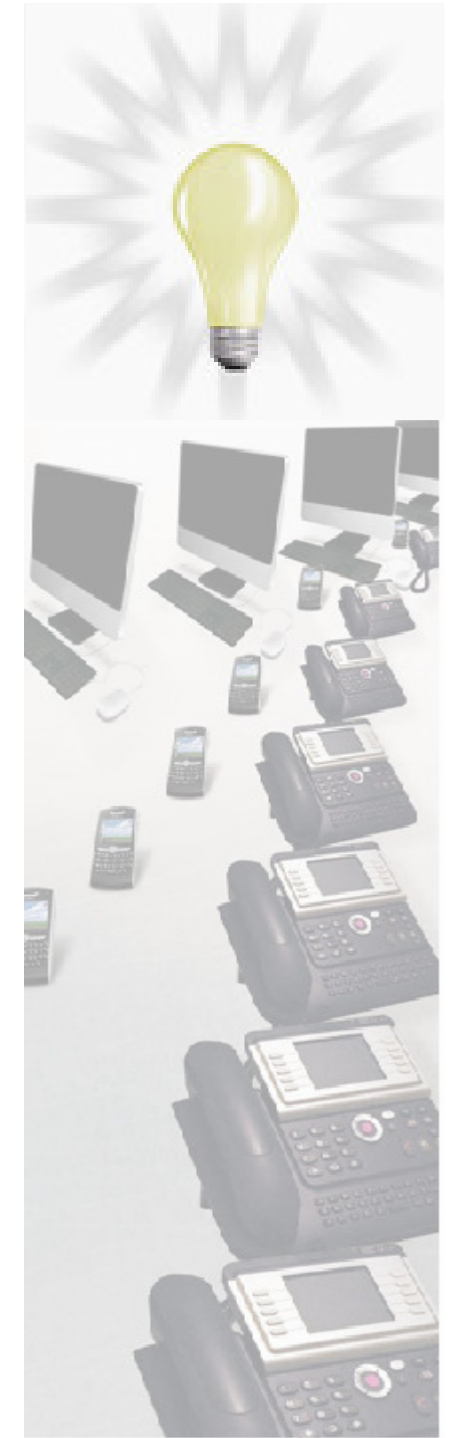
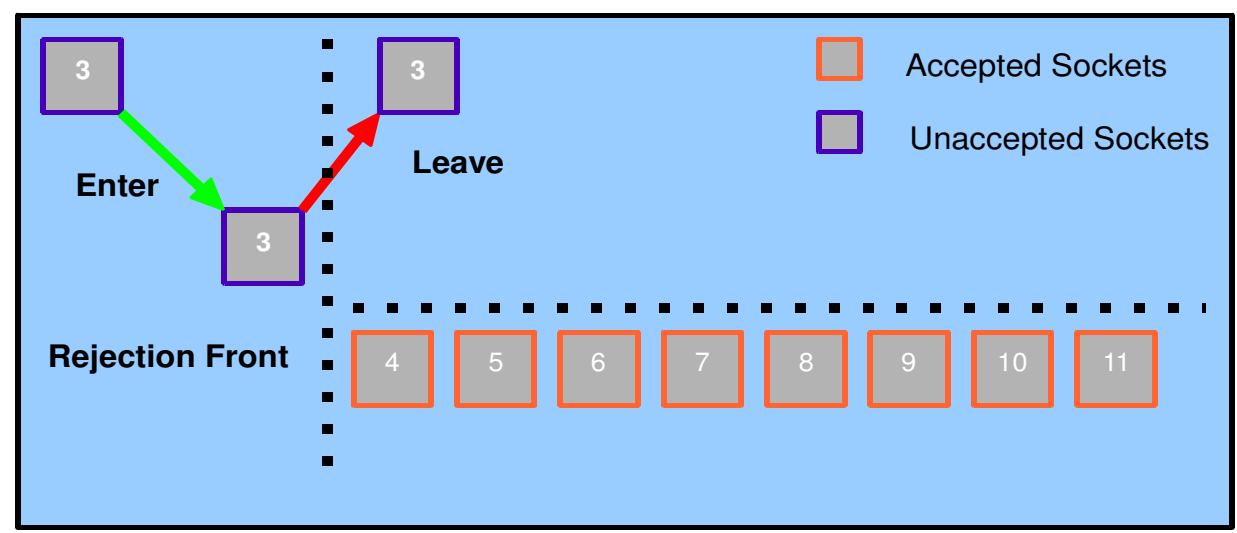
Sleep for X seconds and terminate connections which send data without waiting for the greeting message



# accf\_smtp, DDoS protection for SMTP

## accf\_smtp - how it works

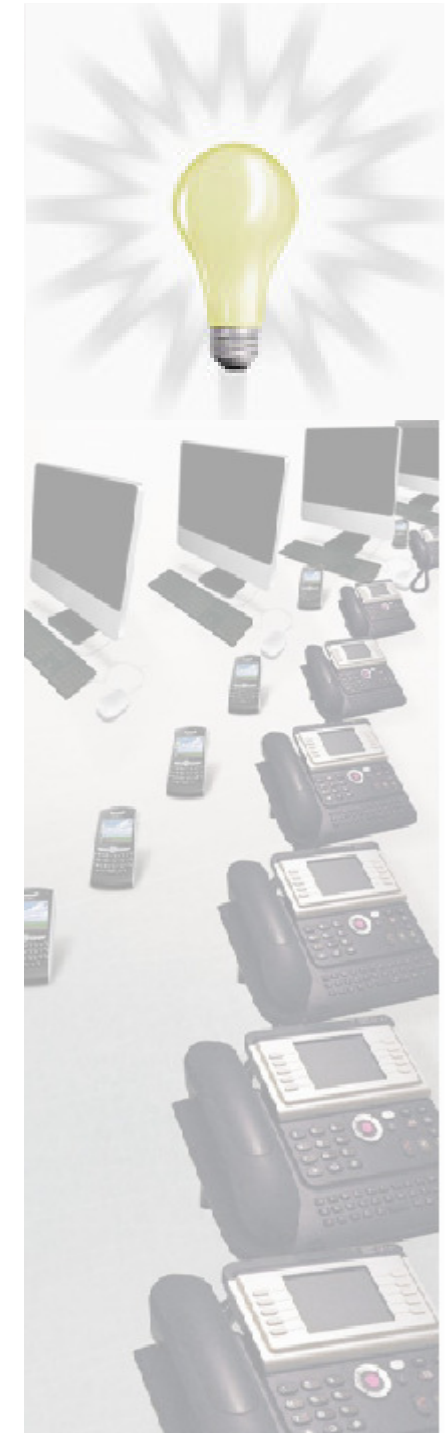
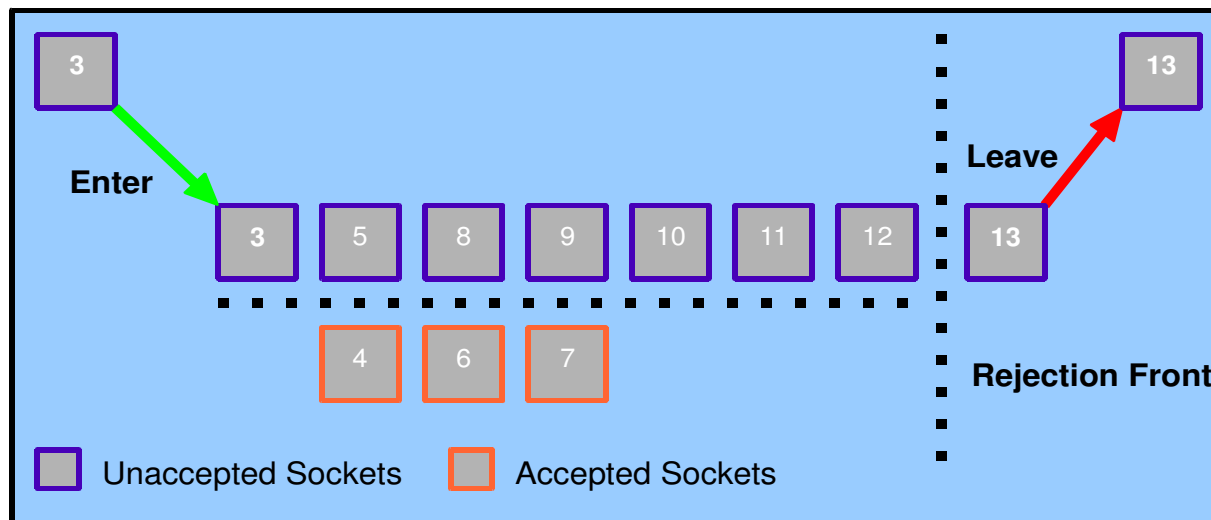
### Traditional way: FIFO queueing mechanism



# accf\_smtp, DDoS protection for SMTP

## accf\_smtp - how it works

### Accept filter way: FILO queueing mechanism



# accf\_smtp, DDoS protection for SMTP

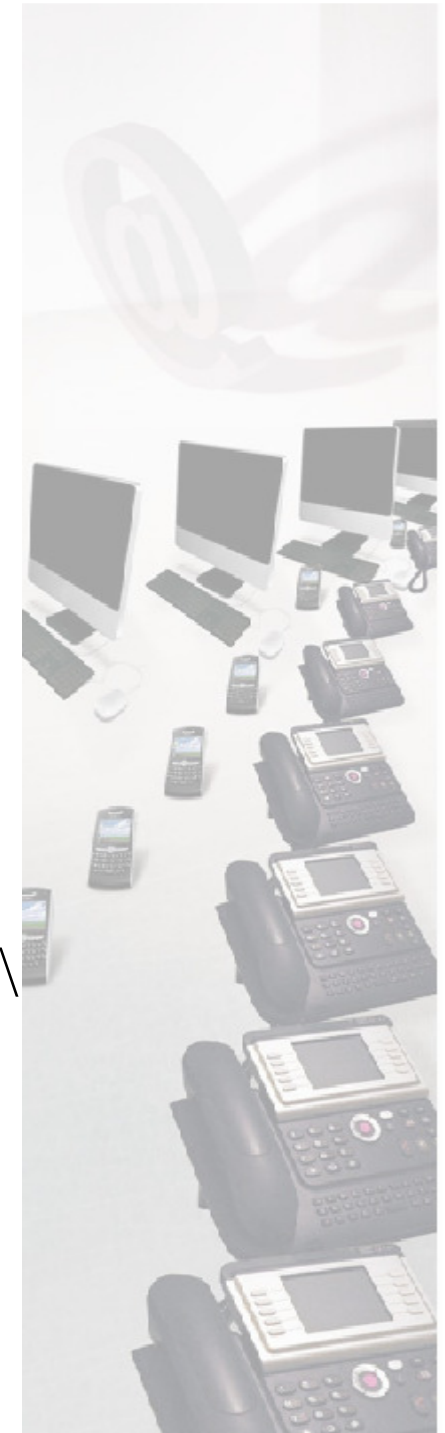
## Dependencies

- **You'll need some Firewall protection:**

- Rate Limiting
- Connection Limiting

- **Example for PF:**

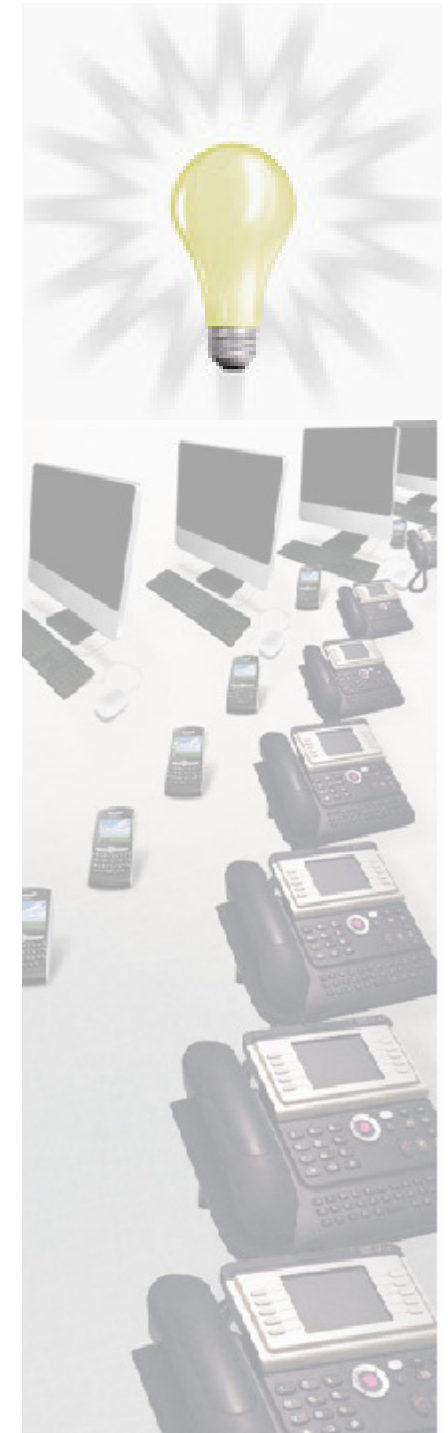
```
pass in quick proto tcp tagged port 25 \  
  flags S/SA keep state \  
  (source-track rule max-src-nodes 10000 max-src-conn 20 \  
  max-src-conn-rate 50/10 overload \  
  <deny_smtp> flush global)
```



# accf\_smtp, DDoS protection for SMTP

## Results:

- The RFC says the sender SHOULD to wait up to 300 seconds for the initial connect ...
- Spammers don't have 300 seconds 😊  
Many of them give up after 10-20 seconds
- Empty connections relating from DDoS attacks are harmless with such an accept filter in place.



# accf\_smtp, DDoS protection for SMTP

## FAQ 1:

**Q: Why BSD ? I use Linux**

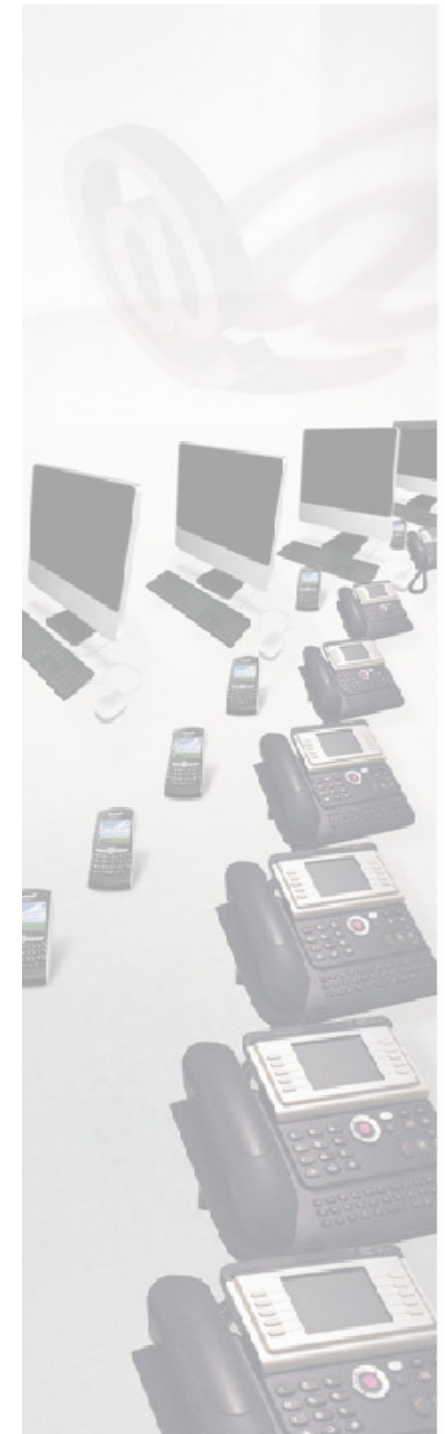
**A:** BSD-Unix's have a wonderful accept-filter API, while Linux is lacking support for this

**Q: Cool, but how can I get this ?**

**A:** It's planed to appear in FreeBSD 8, but maybe not until FreeBSD 9 depending on my workload.

**Q: I need to know more about this**

**A:** No problem, buy the german magazine FreeX/02-2009

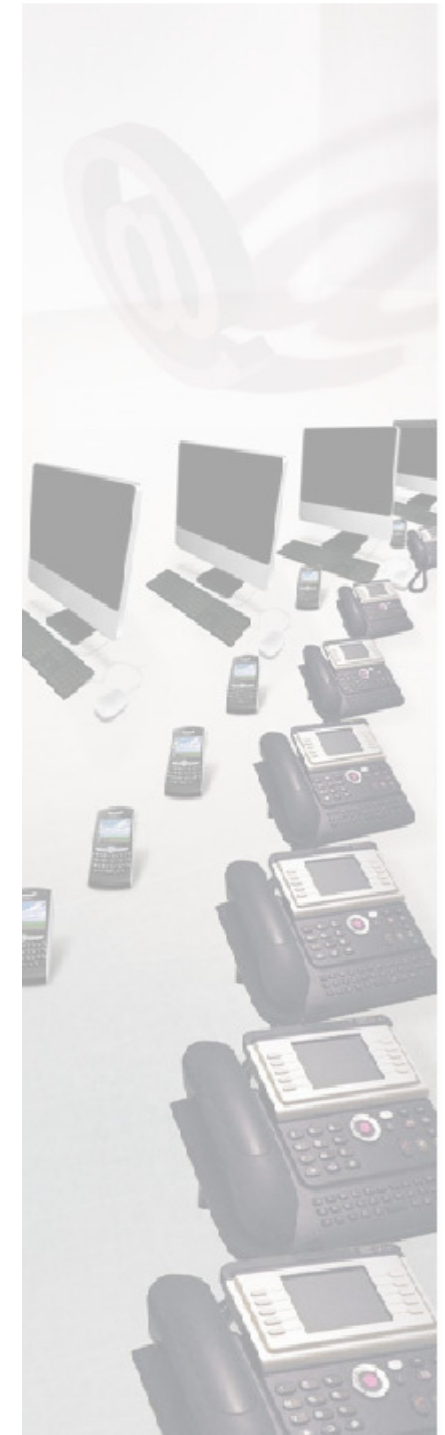


# accf\_smtp, DDoS protection for SMTP

## FAQ 2:

**Q: Does the MTA needs some modifications to run this ?**

**A:** Yes. All MTAs like Sendmail, Postfix, Exim need small patches to activate the accept filter. Loading the kernel module only has no effect at all.



# accf\_smtp, DDoS protection for SMTP

**The end ...**

**Thank you for your attention**

**Enjoy the social event  
and drive carefully !**

**See you @ Swinog 19 !  
( hopefully in a bigger location ;-)**

