LATERAL SECURITY

INFORMATION SECURITY SPECIALISTS

BSD High Availability

Presenter: Sam Banks

Date: 6th April 2011

Company: Lateral Security (IT) Services Limited

LATERAL SECURITY

Company Overview

- Company
  - Lateral Security (IT) Services Limited
  - Founded in April 2008, HQ in Waring Taylor Street, Wellington
  - Directors - Nick von Dadelszen and Ratu Mason
  - Staff - Mark Piper, Sam Banks, Simon Howard, Andrew Kelly, Dean Carter
- Services
  - Information security testing (design, architecture, penetration testing, security controls, policy and compliance)
  - Lifecycle auditing (design, pre prod, post prod)
  - Regular ongoing testing programs
- Differentiators
  - True vendor independence
  - Security testing is our niche specialty
  - Very highly skilled staff

LATERAL | SECURITY

Agenda

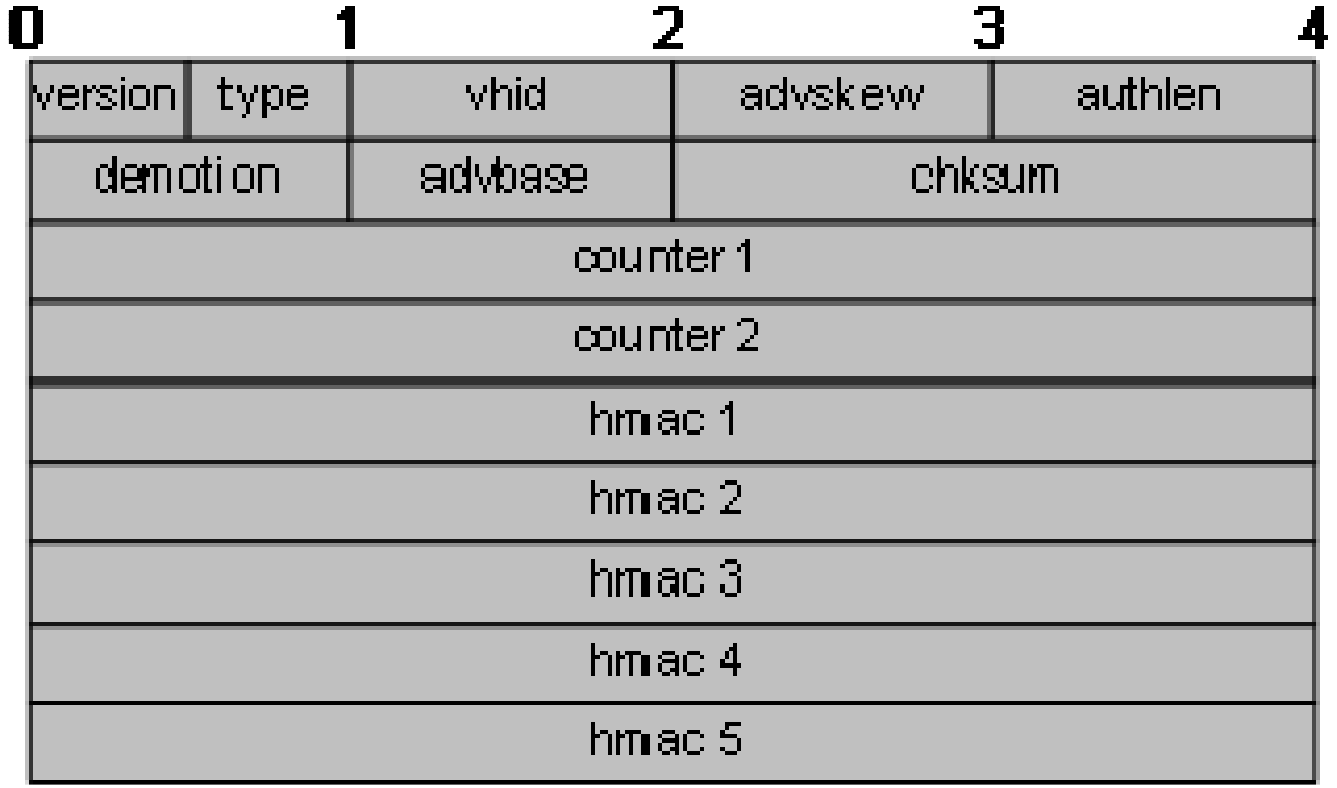
- CARP
- PFSYNC
- No SASYNCD

LATERAL | SECURITY

CARP

- Common Address Redundancy Protocol
- First appeared in OpenBSD in ~2002-2004 (R3.5)
- Provides IP sharing functionality
- Also provides load balancing functionality (ARP and IP)

CARP Protocol



LATERAL | SECURITY

CARP Protocol

- Only active master advertises
- Special Ethernet header in form of
  - 00:00:5e:00:01:<VHID>
- Advertisements are multicast to 224.0.0.18
  - One per advbase seconds + (advskew * 1000000 / 256)

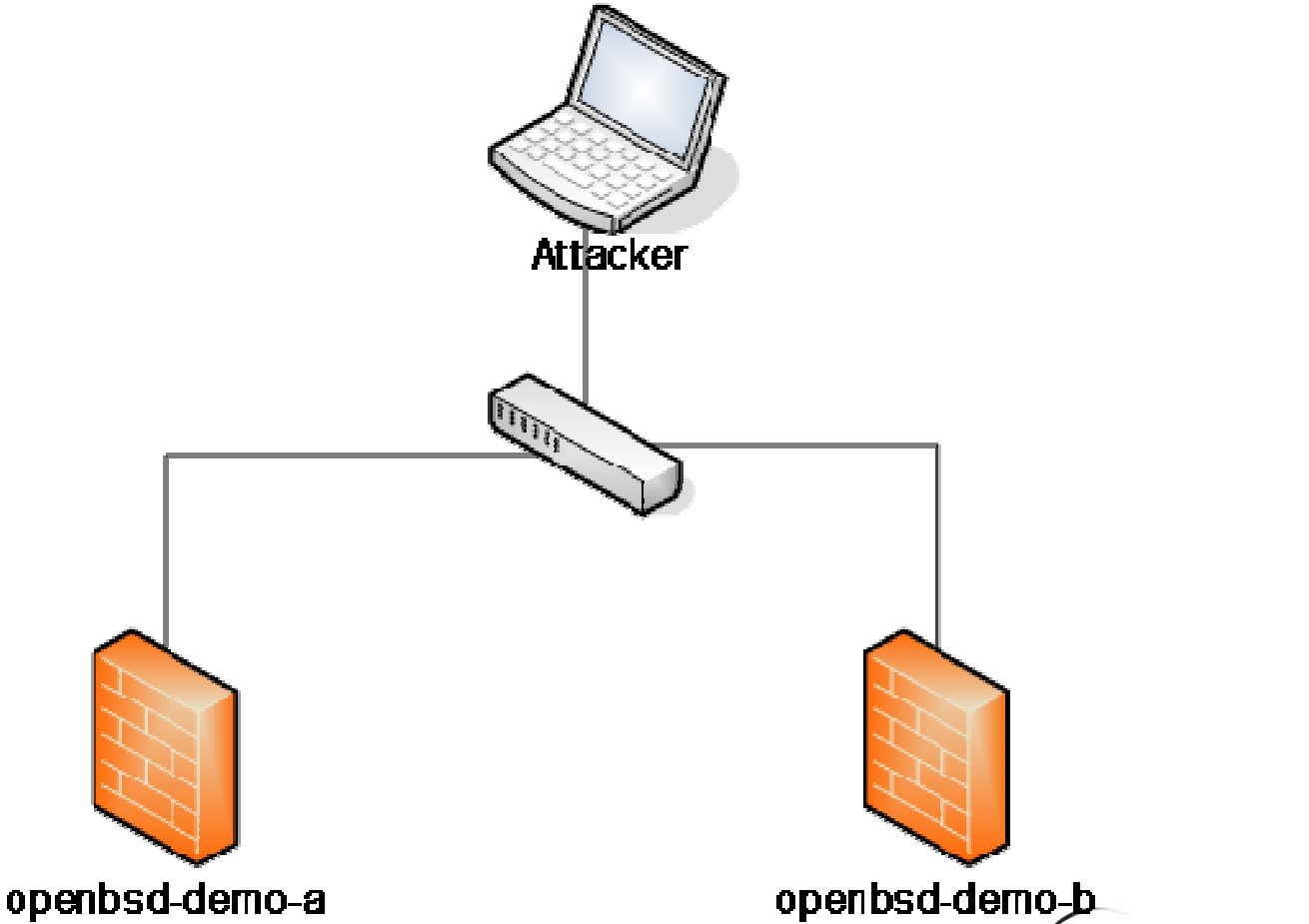
CARP Security

- Shared secret key
- HMAC field contains a SHA1 hash fields including:
  - ipad created from key/pass
  - Version
  - Type
  - VHID
  - MAC if different from default
  - Virtual IP(s)

CARP Attacks

- Force step-down of all CARP nodes

CARP Step-Down Demo



LATERAL | SECURITY

CARP Workarounds/Fixes

- Administrative
  - CARP over IPSEC
- Definite
  - Include all fields in SHA1 hash
  - Decouple advertisements from syncdev interface
- Potential
  - Sync node counters
  - Make step-down harder
  - Update documentation with IPSEC setup

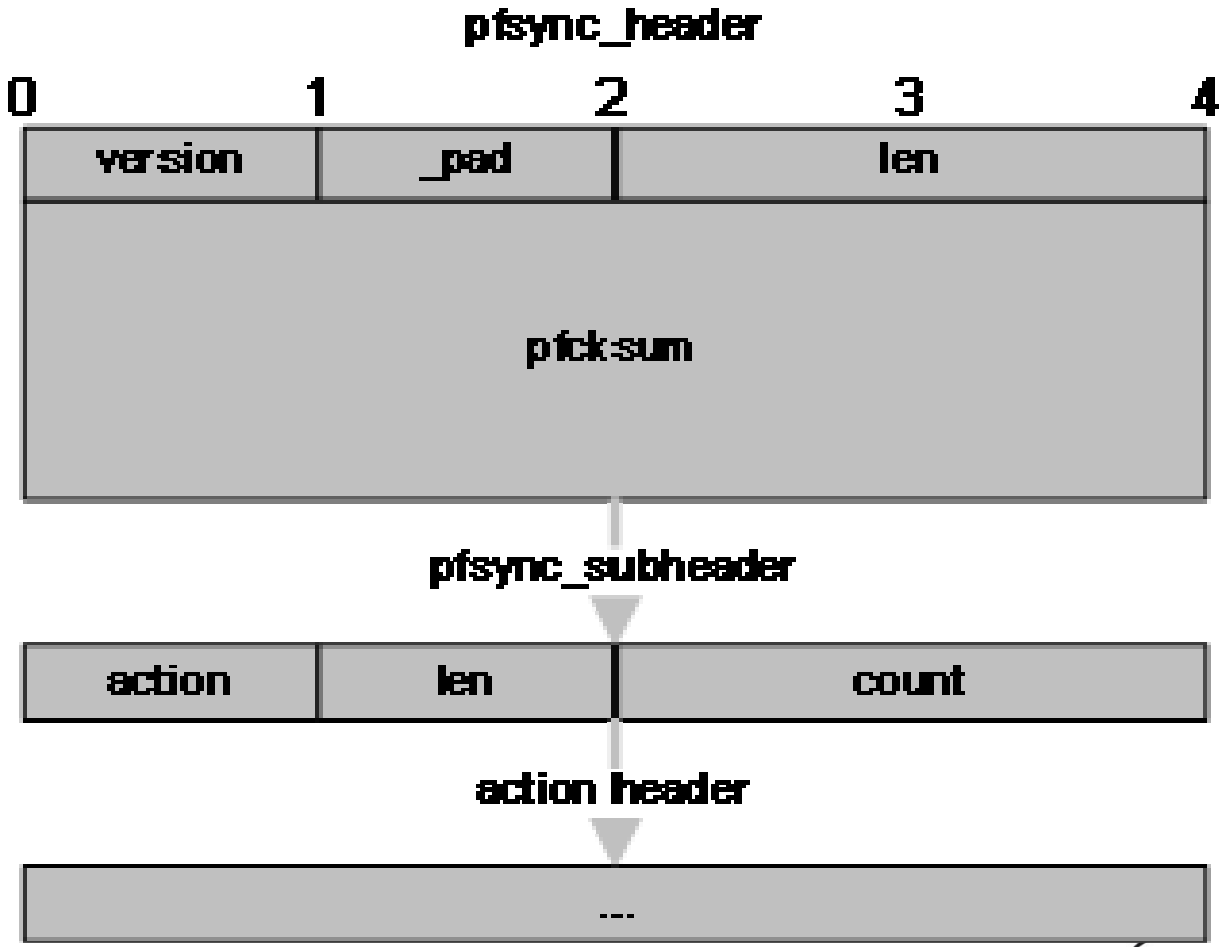
PFSYNC

- Provides PF state sharing between nodes
- Usually used in conjunction with CARP
- Created in 2001-2003 (R3.3)

PFSYNC Protocol

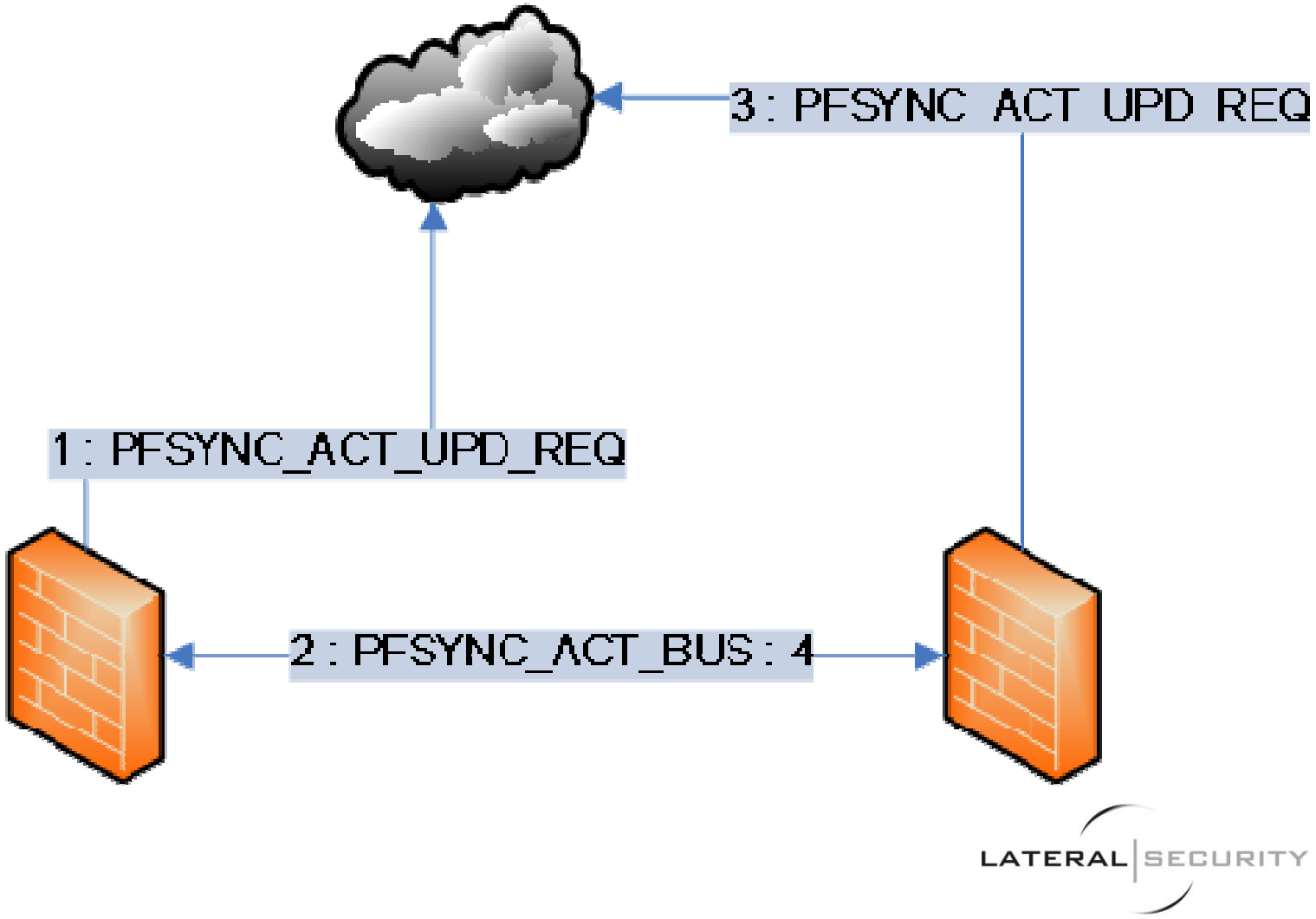
- All packets are multicast to 224.0.0.240
- Packet data sits directly on top of IP
- Reasonably complex protocol

PFSYNC Protocol



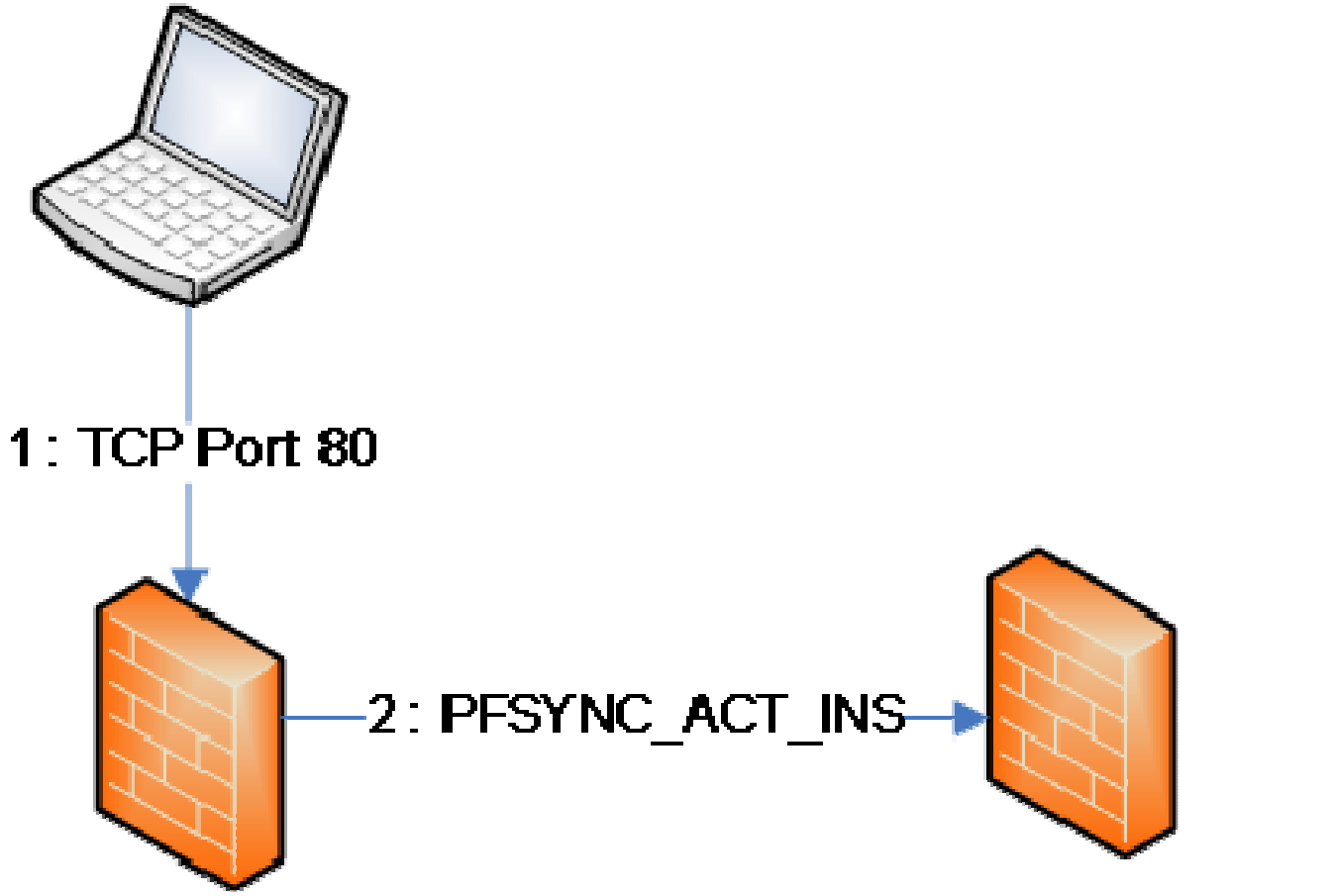
LATERAL | SECURITY

Initialisation



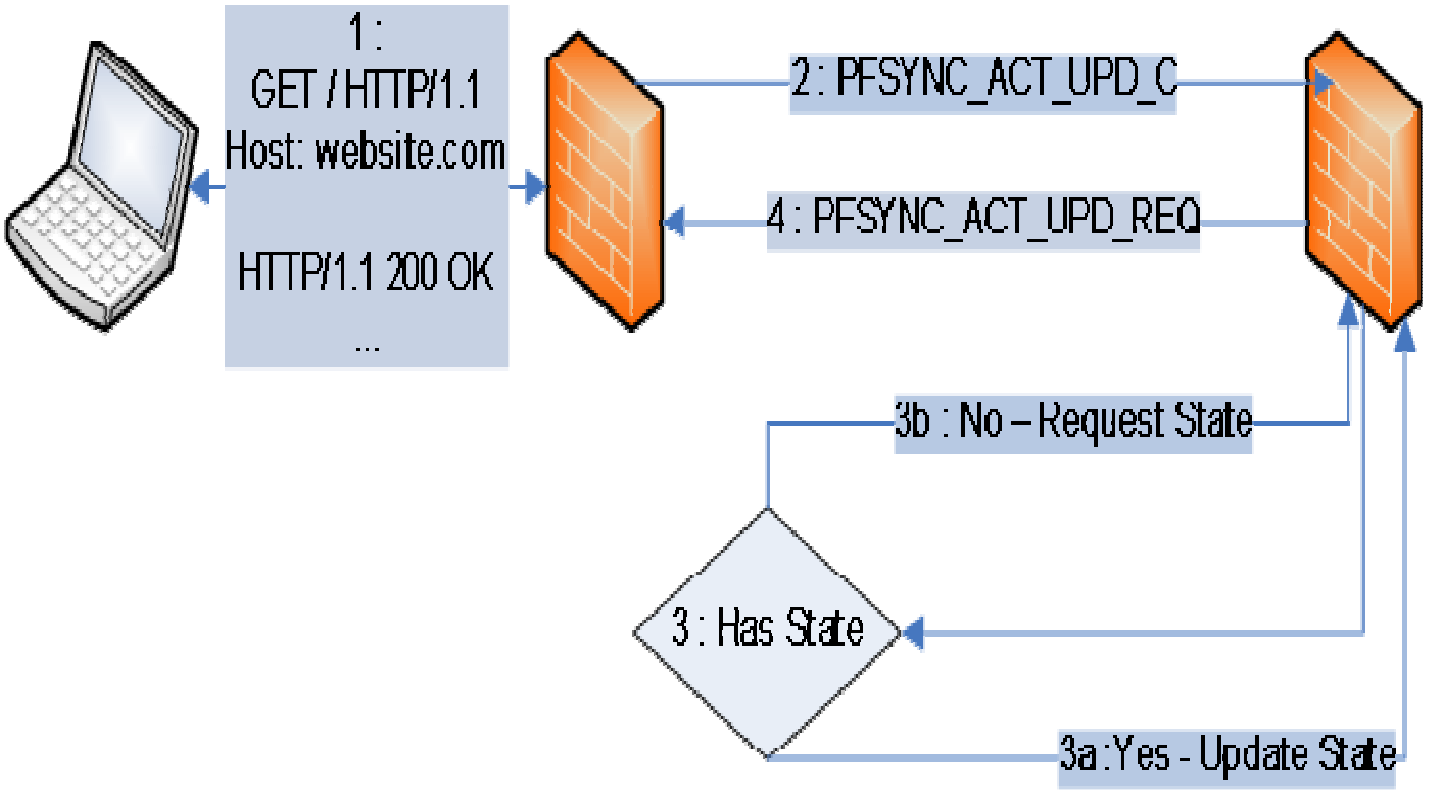
LATERAL | SECURITY

State Insertion



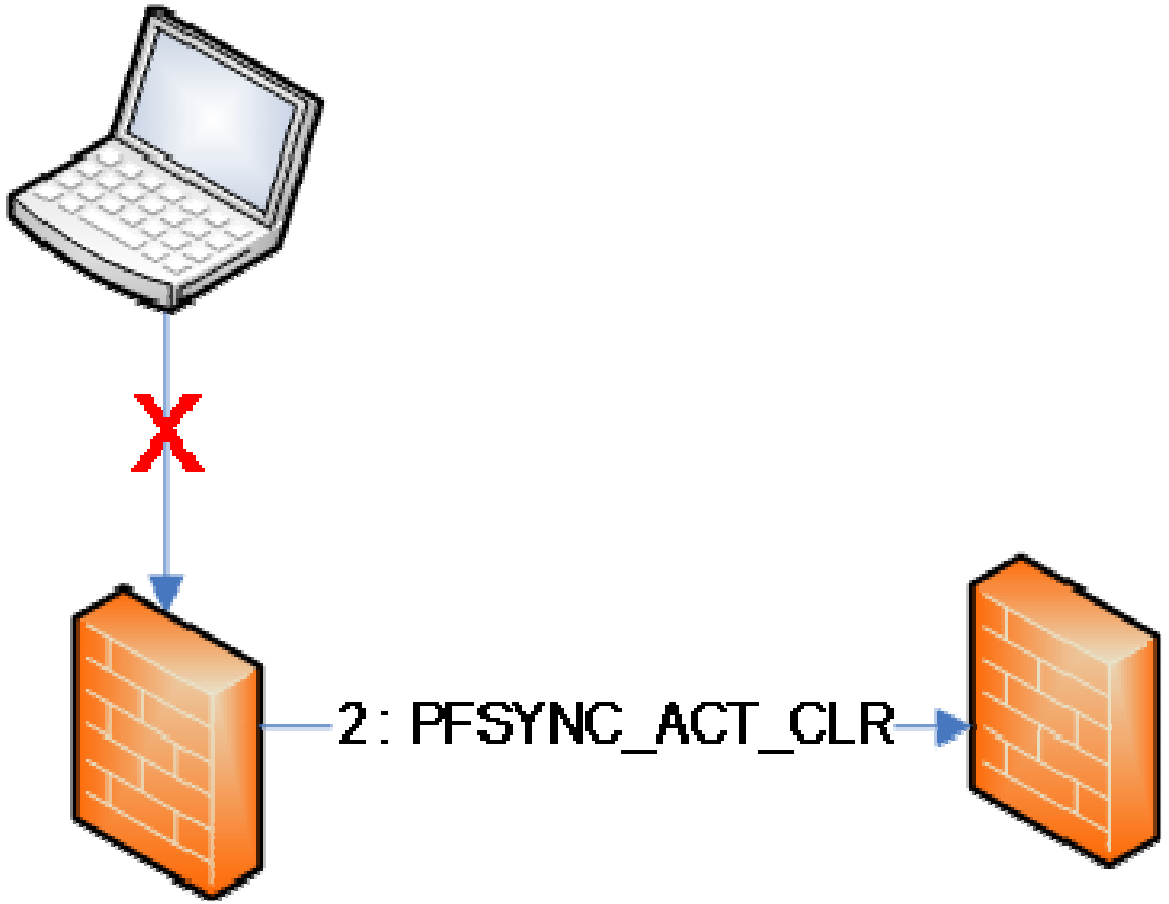
LATERAL | SECURITY

State Update



LATERAL | SECURITY

State Deletion



LATERAL | SECURITY

PFSYNC Security

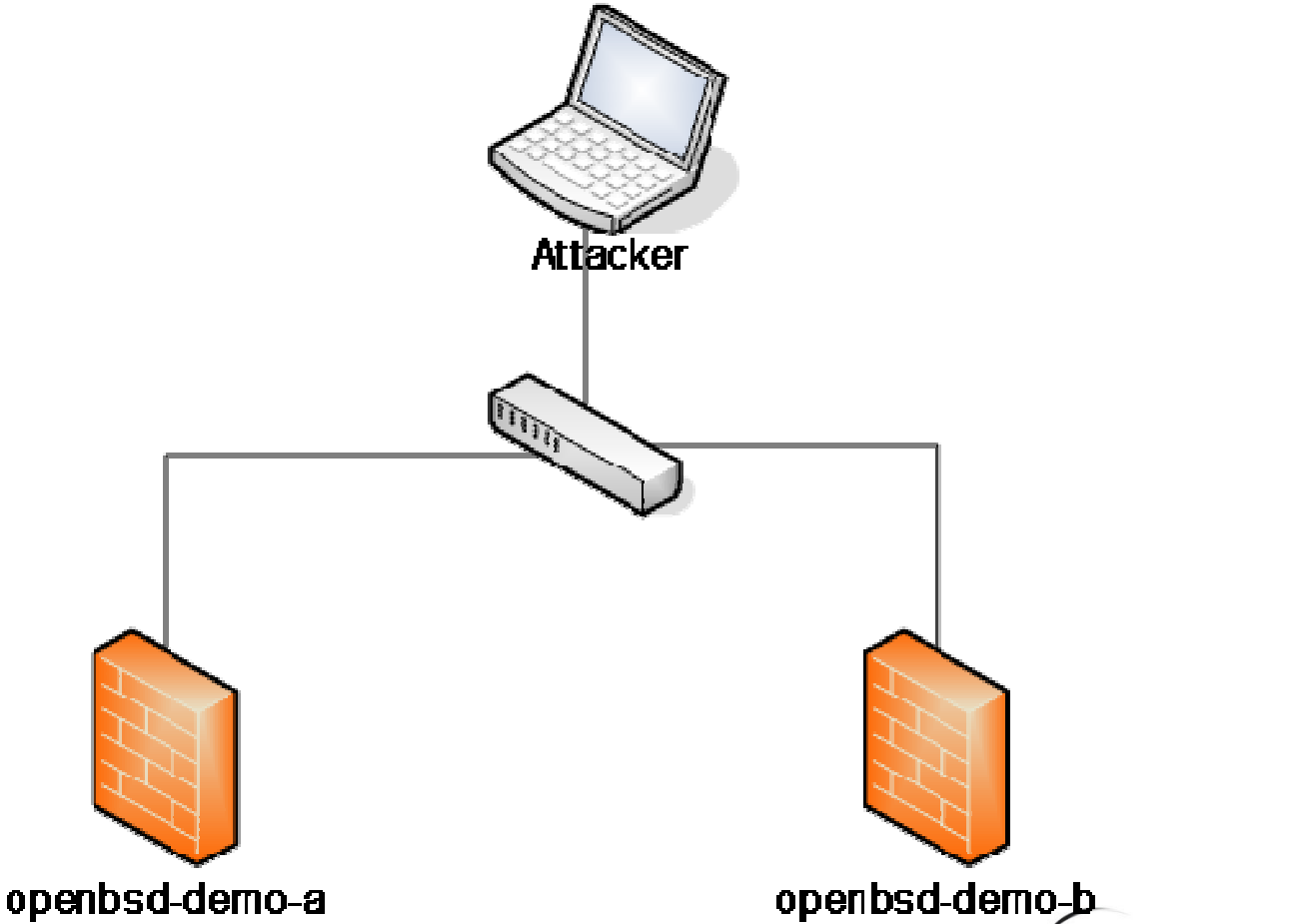
- “It is important that the pfsync traffic be well secured as there is no authentication on the protocol and it would be trivial to spoof packets which create states, bypassing the pf ruleset.”
- In other words, there’s no baked-in security

LATERAL | SECURITY

PFSYNC Attacks

- Basically anything the protocol can do
  - Firewall bypass
  - DoS via state deletion or bogus updates
  - Potential code exec/DoS/whatever bugs?

PFSYNC Demos



LATERAL | SECURITY

PFSYNC Workarounds/Fixes

- Administrative
  - Cross-over the sync nodes
  - Solid Layer 2 security
  - PFSYNC over IPSEC
- Potential:
  - Shared secret packet hashing scheme similar to CARP
  - Man page security section?

LATERAL | SECURITY

Kiwicon(.org)

LATERAL | SECURITY

LATERAL SECURITY

INFORMATION SECURITY SPECIALISTS

Contact Details

sam.banks@lateralsecurity.com

sam.banks.nz@gmail.com

Lateral Security (IT) Services Limited

Wellington

38-42 Waring Taylor Street (level 7, Petherick Tower)

PO Box 8093, Wellington 6143, New Zealand

Phone: +64 4 4999 756

Email: sas@lateralsecurity.com

Auckland

187 Queen Street (level 8, Landmark House)

PO Box 7706, Auckland, New Zealand

Phone: +64 9 3770 700

Email: sas@lateralsecurity.com

LATERAL SECURITY