



# pfSense: Die Firewall- & Routing-Lösung für Unternehmen

15. November 2013



Michael Steinfurth  
Linux/Unix Consultant & Trainer  
B1 Systems GmbH  
steinfurth@b1-systems.de

# Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source Themen
- national & international tätig
- über 60 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- dezentrale Strukturen

# Schwerpunkte

- Virtualisierung (XEN, KVM & RHEV)
- Systemmanagement (Spacewalk, Red Hat Satellite, SUSE Manager)
- Konfigurationsmanagement (Puppet & Chef)
- Monitoring (Nagios & Icinga)
- IaaS Cloud (OpenStack & SUSE Cloud)
- Hochverfügbarkeit (Pacemaker)
- Shared Storage (GPFS, OCFS2, DRBD & CEPH)
- Dateiaustausch (ownCloud)
- Paketierung (Open Build Service)
- Administratoren oder Entwickler zur Unterstützung des Teams vor Ort

# Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**

# Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**

# Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**

# Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**

## Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**



## Werdegang von pfSense

- 2004: Projektstart als Fork von **M0n0wall** (BSD Lizenz)
- 2004: Gründer sind Scott Ullrich & Chris Buechler
- 2007: Gründungsjahr **BSD Perimeter**
- 2007: Startschuss für kommerziellen Support
- 2013: Release von pfSense 2.1 liefert nativen IPv6 Support
- 2013: BSD Perimeter wird zu **Electric Sheep Fencing**

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen



# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# pfSense

- ist eine FreeBSD-basierte Routing- & Firewall-Plattform
- Projektschwerpunkte
  - Server-Hardware
  - Enterprise Features
  - Flexibilität
- Embedded Images verfügbar (bspw. für PCEngines ALIX)
- Stand April über 167.000+ Live Deployments
- aktive Community von Entwicklern
- theoretisch unlimitierte Anzahl an Netzwerkschnittstellen

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)



# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

# Enterprise Features 1/2

- DHCP Server & DNS Forwarder
- VLANs & QinQ (IEEE 802.1q, 802.1ad)
- Link Aggregation (IEEE 802.3ad)
- CARP, ähnlich VRRP (RFC 5798)
- Tunnel-Protokolle & „Pseudo Wire“
  - OpenVPN, IPSEC, PPTP
  - GRE, GIF, PPP, PPPoE
- OSPFv3 & BGPv4 (via Quagga)

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4



## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Enterprise Features 2/2

- Network Address Translation
- Traffic Shaping
- Gateway-Gruppen
  - Failover & Load Sharing
  - Policy-basiertes Routing
- OS Fingerprinting
- Deep Packet Inspection
- Captive Portal, RADIUS, DynDNS
- natives IPv6 & NDP, NPt, Broker, 6to4

## Was pfSense (noch) nicht kann ...

- MPLS – Multi Protocol Label Switching
- TE – Traffic Engineering Tunneling
- VPLS – Virtual Private LAN Service
- SSTP – Secure Socket Tunneling Protocol
- EoIP – Ethernet over IP Tunneling

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting



# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# WebConfigurator

- primäres Werkzeug zur Administration
- Plattform basiert auf **lighttpd** und **PHP**
- flexibel durch XML-basiertes Konfigurations-Backend
- Features:
  - Multi-Benutzer-Fähigkeit inkl. Unterstützung für LDAP
  - Rollenbasierte Zugriffskontrolle (RBAC)
  - Integrierte Zertifikatsverwaltung (ITU-T X.509)
  - Alias-Verwaltung inklusive Autovervollständigung
  - unmittelbarer Zugriff auf Tools für Troubleshooting

# 2.1-RELEASE

webConfigurator pfs01.fw.example.com

Status: Dashboard ?

## pfSense

**Gateways**

Name	RTT	Loss	Status
<b>200.33.20.25</b>			
ISPLEASE1	91.9ms	0.0%	Online
<b>94.23.51.19</b>			
ISP2DIALUP	322ms	0.0%	Online
<b>172.16.19.1</b>			
LAN	0.2ms	0%	Online
<b>10.10.40.2</b>			
DMZ	0.2ms	0%	Online

**System Information**

Name	pfs01.fw.example.com
Version	2.1-RELEASE (amd64) built on Wed Sep 11 18:17:48 EDT 2013 FreeBSD 8.3-RELEASE-p11
Platform	pfSense

**OpenVPN**

**vpn.example.com TCP:1194 Client connections**

Name/Time	Real/Virtual IP
client01	xx.xx.xx.xx:37440
Wed Nov 13 20:04:31 2013	xx.xx.xx.xx

**voipvpn.example.com UDP:8000 Client connections**

Name/Time	Real/Virtual IP
voip01	xx.xx.xx.xx:1194
Wed Nov 13 01:56:30 2013	xx.xx.xx.xx

Abbildung: Dashboard

# 2.1-RELEASE

webConfigurator

pf501.fw.example.com

System: High Availability Sync



**State Synchronization Settings (pfsync)**

Synchronize States

pfsync transfers state insertion, update, and deletion messages between firewalls. Each firewall sends these messages out via multicast on a specified interface, using the PFSYNC protocol (IP Protocol 240). It also listens on that interface for similar messages from other firewalls, and imports them into the local state table.

This setting should be enabled on all members of a failover group.

NOTE: Clicking save will force a configuration sync if it is enabled! (see Configuration Synchronization Settings below)

---

Synchronize Interface

If Synchronize States is enabled, it will utilize this interface for communication.  
 NOTE: We recommend setting this to a interface other than LAN! A dedicated interface works the best.  
 NOTE: You must define a IP on each machine participating in this failover group.  
 NOTE: You must have an IP assigned to the interface on any participating sync nodes.

---

pfsync Synchronize Peer IP

Setting this option will force pfsync to synchronize its state table to this IP address. The default is directed multicast.

---

**Configuration Synchronization Settings (XMLRPC Sync)**

Synchronize Config to IP

Enter the IP address of the firewall to which the selected configuration sections should be synchronized.

NOTE: XMLRPC sync is currently only supported over connections using the same protocol and port as this system - make sure the remote system's port and protocol are set accordingly!

NOTE: Do not use the Synchronize Config to IP and password option on backup cluster

Abbildung: H/A Konfiguration

## 2.1-RELEASE

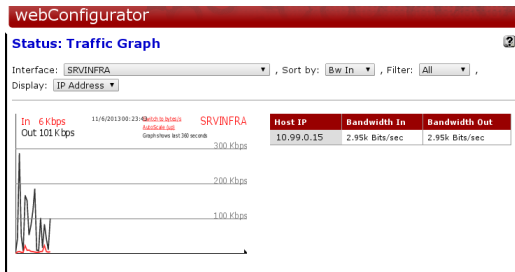


Abbildung: Echtzeit-Statistiken



# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt

# Kommandozeile

- Kommandozeilenzugriff
  - physikalisch via Terminal
  - serieller Port (abhängig von Hardware)
  - via Netzwerk & Secure Shell (SSH)
- Troubleshooting erfordert meist erfahrenen BSD/UNIX Admin
- Menüführung ermöglicht Zugriff auf wichtigste Funktionen
- Konfigurationsänderungen nur via PHP (Konsistenz)
- Telnet wird nicht unterstützt



## Kommandozeilen-Menü

```
$ ssh root@pfs01.lab.b1-systems.de
*** Welcome to pfSense 2.1-RELEASE-pfSense (amd64) on pfs01 ***

ISP1LEASE (wan) -> lagg0_vlan50 -> v4: 200.33.20.24/28
LAN (lan)        -> lagg0_vlan1001 -> v4: 172.16.19.2/16
ISP2DIALUP (opt1) -> pppoe0      -> v4/PPPoE: 94.23.51.20/32
DMZ (opt2) -> lagg0_vlan501 -> v4: 10.10.40.0/24

0) Logout (SSH only)          8) Shell
1) Assign Interfaces          9) pfTop
2) Set interface(s) IP address 10) Filter Logs
3) Reset webConfigurator password 11) Restart webConfigurator
4) Reset to factory defaults   12) pfSense Developer Shell
5) Reboot system              13) Upgrade from console
6) Halt system                14) Disable Secure Shell (sshd)
7) Ping host                  15) Restore recent configuration

Enter an option:
```

# Anwendungsfälle

# H/A Firewall Cluster

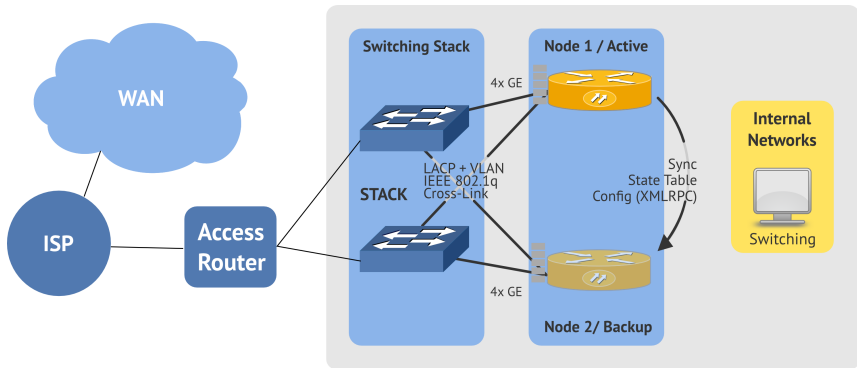


Abbildung: H/A Setup inkl. Switching Stack und Link Aggregation

# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)



# H/A Firewall Cluster

- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

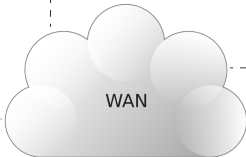
- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# H/A Firewall Cluster

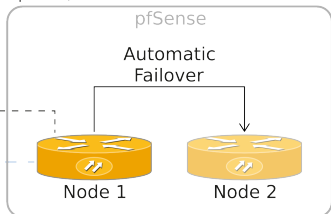
- maximal zwei Knoten (N+1)
- transparenter Failover von aktiven Verbindungen
- kein Load Sharing auf IP Layer (Active/Passive)
  - Traffic läuft ausschließlich über aktiven Knoten
- Technologien
  - **CARP** – H/A auf IP Layer mit virtuellen IPs
  - **pfsync** – State Table Replikation (Verbindungen)
  - **XMLRPC** – Replikation der pfSense-Konfiguration (HTTP/S)

# VPN Appliance

pfSense, Cisco, Juniper, Checkpoint [...]



OpenVPN/IPSEC



# VPN Appliance 1/2

- **Anwendungsfälle**
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten



# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

# VPN Appliance 1/2

- Anwendungsfälle
  - Roadwarrior → Anbindung mobiler Endgeräte
  - Site-to-Site → standortübergreifende Anbindung
- ermöglicht verschlüsselten Zugriff auf Infrastruktur
- Parallelbetrieb von OpenVPN und IPSEC
- Betrieb im H/A Cluster kein Problem (Active/Passive)
  - kein Load Sharing auf IP Layer
  - kein transparenter Failover von aktiven VPN-Sitzungen, da unterbrochen bei Ausfall des aktiven Knoten

## VPN Appliance 2/2

- Unterstützung für Crypto-Engines (FreeBSD)
  - Intel AES-NI (ab FreeBSD 9)
  - HiFn PowerCrypt, 97XX, 77XX [..]
  - AMD Geode LX (Embedded)
- maximale Benutzeranzahl hardwareabhängig

## VPN Appliance 2/2

- Unterstützung für Crypto-Engines (FreeBSD)
  - Intel AES-NI (ab FreeBSD 9)
  - HiFn PowerCrypt, 97XX, 77XX [..]
  - AMD Geode LX (Embedded)
- maximale Benutzeranzahl hardwareabhängig

## VPN Appliance 2/2

- Unterstützung für Crypto-Engines (FreeBSD)
  - Intel AES-NI (ab FreeBSD 9)
  - HiFn PowerCrypt, 97XX, 77XX [..]
  - AMD Geode LX (Embedded)
- maximale Benutzeranzahl hardwareabhängig

## VPN Appliance 2/2

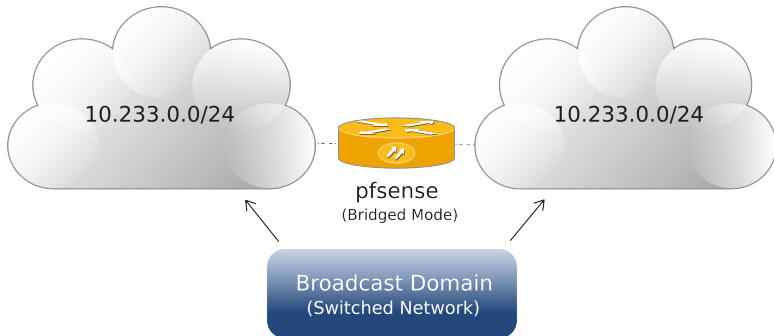
- Unterstützung für Crypto-Engines (FreeBSD)
  - Intel AES-NI (ab FreeBSD 9)
  - HiFn PowerCrypt, 97XX, 77XX [..]
  - AMD Geode LX (Embedded)
- maximale Benutzeranzahl hardwareabhängig



## VPN Appliance 2/2

- Unterstützung für Crypto-Engines (FreeBSD)
  - Intel AES-NI (ab FreeBSD 9)
  - HiFn PowerCrypt, 97XX, 77XX [..]
  - AMD Geode LX (Embedded)
- maximale Benutzeranzahl hardwareabhängig

# Transparente Firewall



# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!



# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

# Transparente Firewall

- passive Filterung in „geswitchten“ Netzen
- zusätzlicher Schutz für Broadcast-basierte Dienste
- Firewall:
  - benötigt keine IP-Adresse im zu filternden Netz
  - „passiv“, da aktiv kein Routing involviert
- einfache Restriktion auf Layers 2-4 (ETHER,IP,PORT)
- kostengünstige Möglichkeit Netze abzusichern
- keine Anpassung der IP-Konfiguration erforderlich!

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an [info@b1-systems.de](mailto:info@b1-systems.de)  
oder +49 (0)8457 - 931096