

# Netzwerkadministration

mit der



netsecdb

Herzlich Willkommen!

- Server, Firewalls und Router sind ständigen Angriffen ausgesetzt.
- DoS-Attacken (Denial of Service) legen immer öfter Netze lahm (Beispiele: internetx, twitter)
- SPAM's fressen den Löwenanteil der Bandbreite im Bereich Kommunikation und sind „timebandits“ (arbeitstechnische Zeiträuber)
- Einbruchsversuche auf Webserver nehmen ständig zu
- Bruteforce-Angriffe (programmgestütztes Ausprobieren aller Varianten oder bestimmter ausgewählter Standard Logins) auf ftp und ssh-services sind an der Tagesordnung

- Es häufen sich die Meldungen über das Eindringen in staatliche/industrielle Sicherheitsbereiche zur illegalen Beschaffung von Informationen (Forschung, Kreditkarten, Transaktionsdaten etc.)
- Zu viele Server mit Internetdiensten werden 'gehackt' (im Besitz inkl. voller Adminrechte übernommen)
- Das 'mobile Arbeiten' unterläuft vielfach sämtliche netzwerktechnisch festgelegten Sicherheitsrichtlinien.
- Immer mehr Programme auf Arbeitsplatzrechnern 'telefonieren nach Hause' – meist unkontrolliert
- Viele Netzwerke sind durch s.g. 'Bots' verseucht



# Einbruchversuche in Webseiten:

In 365 Tagen über 222.000 mal auf die  
netsecdb.de.



# Einbrüche ... per exploit.

Die Anleitung dazu:

**Dr. Wolfgang Schäuble MdB**  
Bundesminister des Innern

CDU/CSU-Bundestagsfraktion, CDU-Deutschland

**VISIT:**  
--> Vorratsdatenspeicherung <---

**Geschlossene Gesellschaft - Integration gescheitert**  
02.02.2009 | Bundesminister Dr. Wolfgang Schäuble diskutiert in der Bundung 24Life im ZDFR Fernsehen

**„Täterforschung im globalen Kontext“**  
27.01.2009 | Peak von Bundesminister Dr. Wolfgang Schäuble zur Eröffnung der internationalen Konferenz in Berlin

**Religionen und ethische Verantwortung in einer globalisierten Welt**  
11.01.2009 | Die Balance immer wieder neu gewinnen

**MILWORM**

Exploit-ID	Exploit Name	Exploit Type	Exploit Date	Exploit Status
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready
2009-01-01	Microsoft Exchange Mailbox Enumeration	Enumeration	2009-01-01	Ready

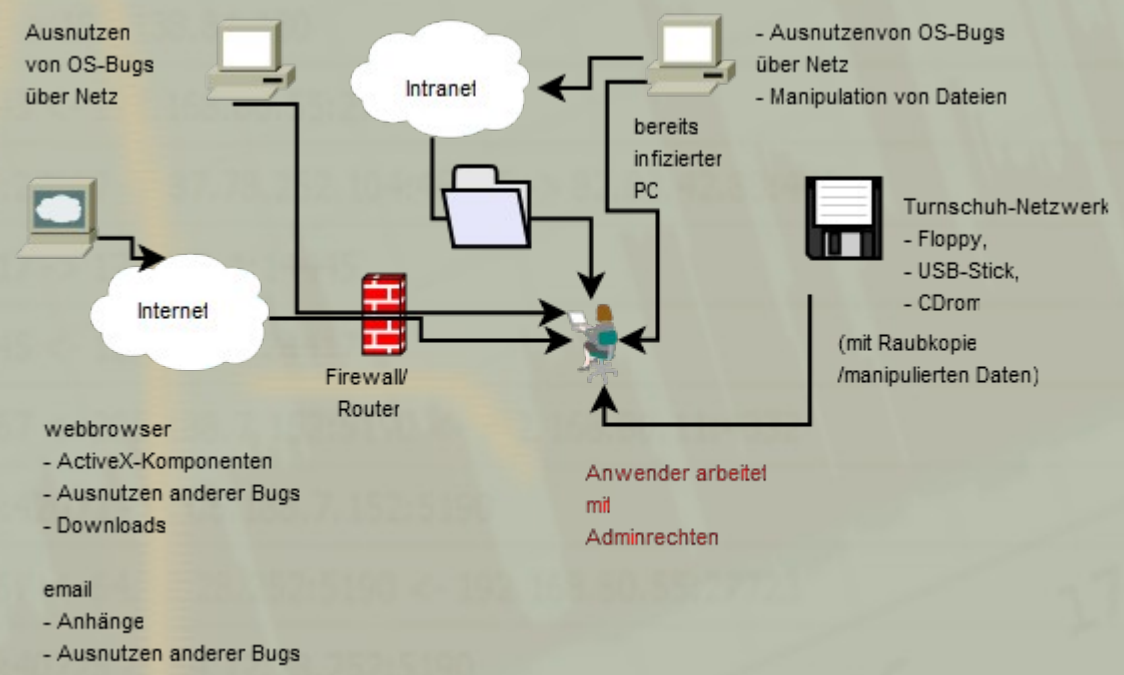
In den wenigsten Fällen werden Server mit Internetdiensten durch Firewalls geschützt.

Um Arbeitszeit zu sparen, werden viele durch Firewalls geschützte Netze mit einer zu 'liberalen' Policy betrieben:

- von außen kommende Pakete verboten
- von innen abgehende Pakete erlaubt
- einige wenige Protokollfilter

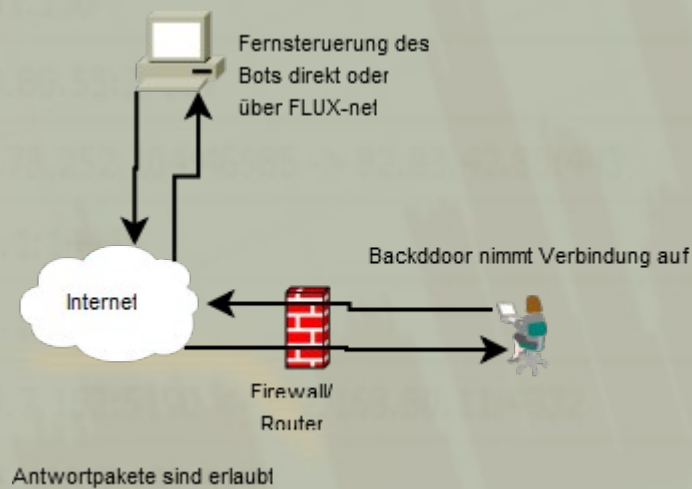
# Schwachstellen 'liberaler' Policies:

## - Infektionswege -



# Schwachstellen 'liberaler' Policies:

- Eindringen ins Netz -



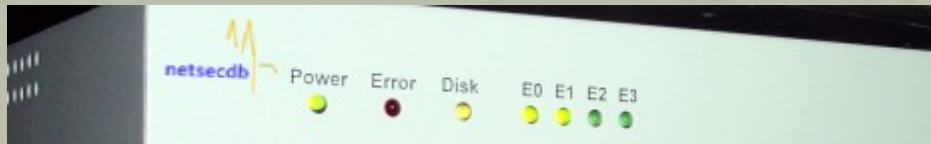
## Firewalls mit Features wie

- High-Availibility (Hochverfügbarkeit),
- Transparenter DMZ (vor und hinter der Firewall gleiche Netzbereiche, weil man kein eigenes Segment verfügbar hat.),
- unlimitierten VPN-Zugängen,
- Statistischer Auswertung,
- Austausch der Konfigurationen untereinander,
- u.s.w.

... sind unverschämt teuer oder bezahlbar bei Erstkauf werden aber schnell durch ansteigende Lizenzkosten für sogenannte 'Software-Optionen' zum Geldfresser.

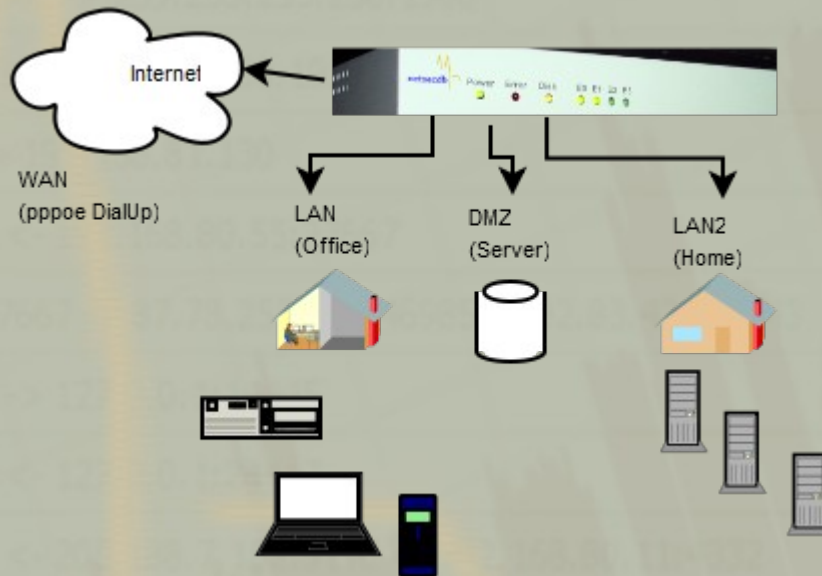
Die Hersteller verkaufen sie nur über ihre zertifizierten/lizenzierten Wiederverkäufer.

Was ist das?



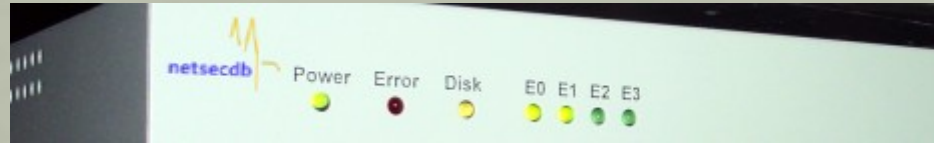
Eine Firewall.

... lässt sich im Home-Office einsetzen:

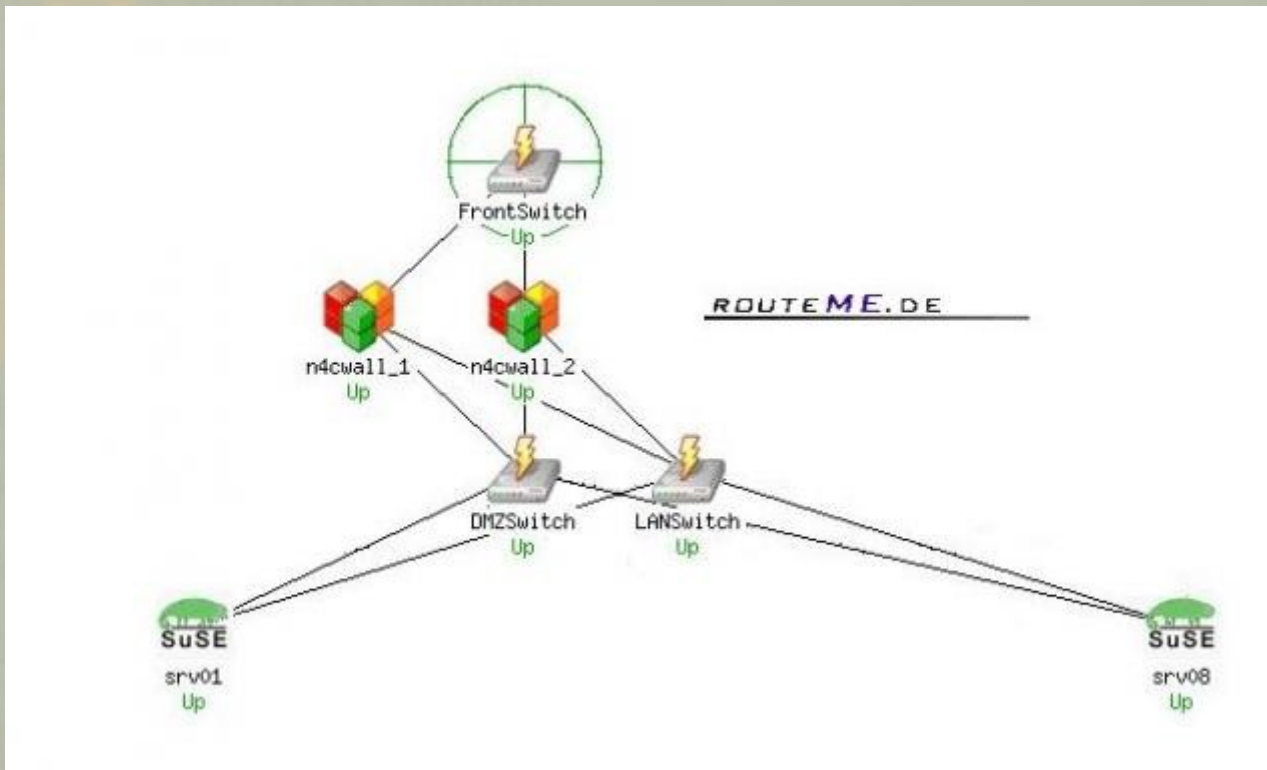


...inkl. Zugriffskontrolle  
und Inhaltsfilterung  
für den Jugendschutz,

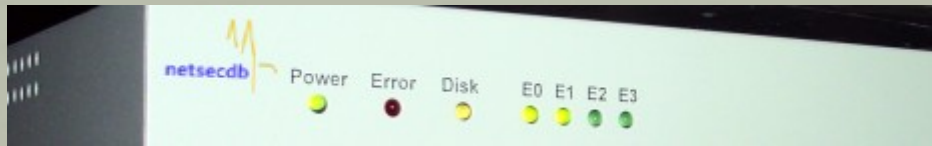




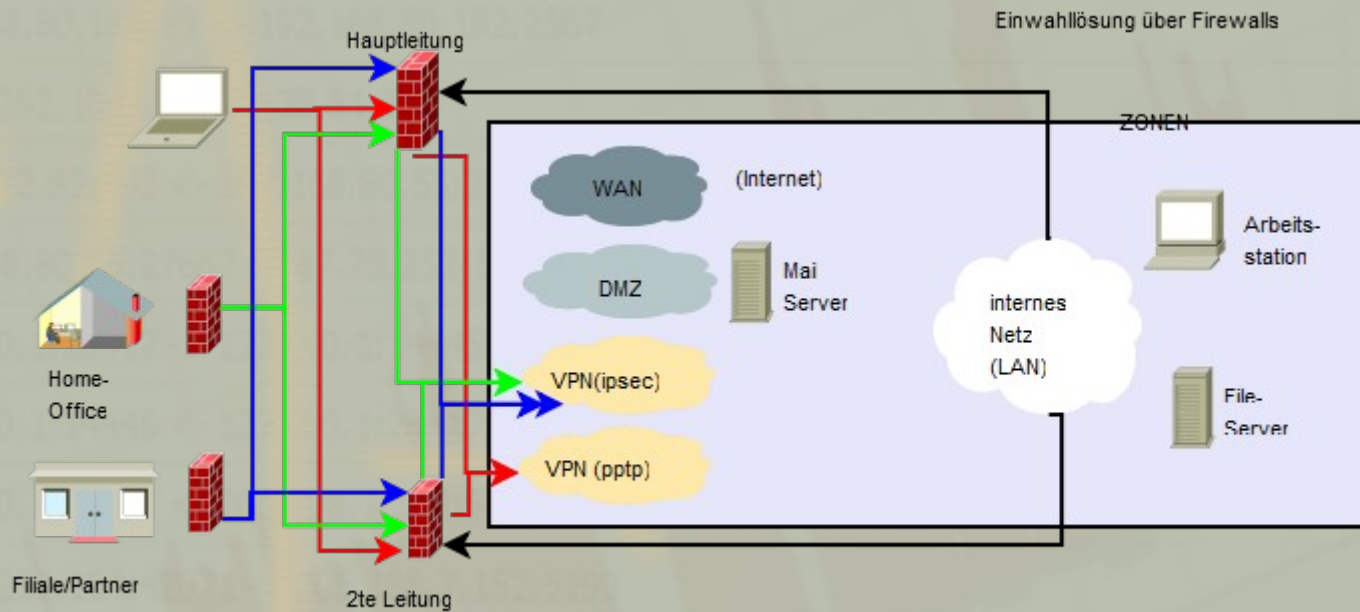
... im Rechenzentrum:



...wo Redundanz und Lastverteilung besonders wichtig ist..



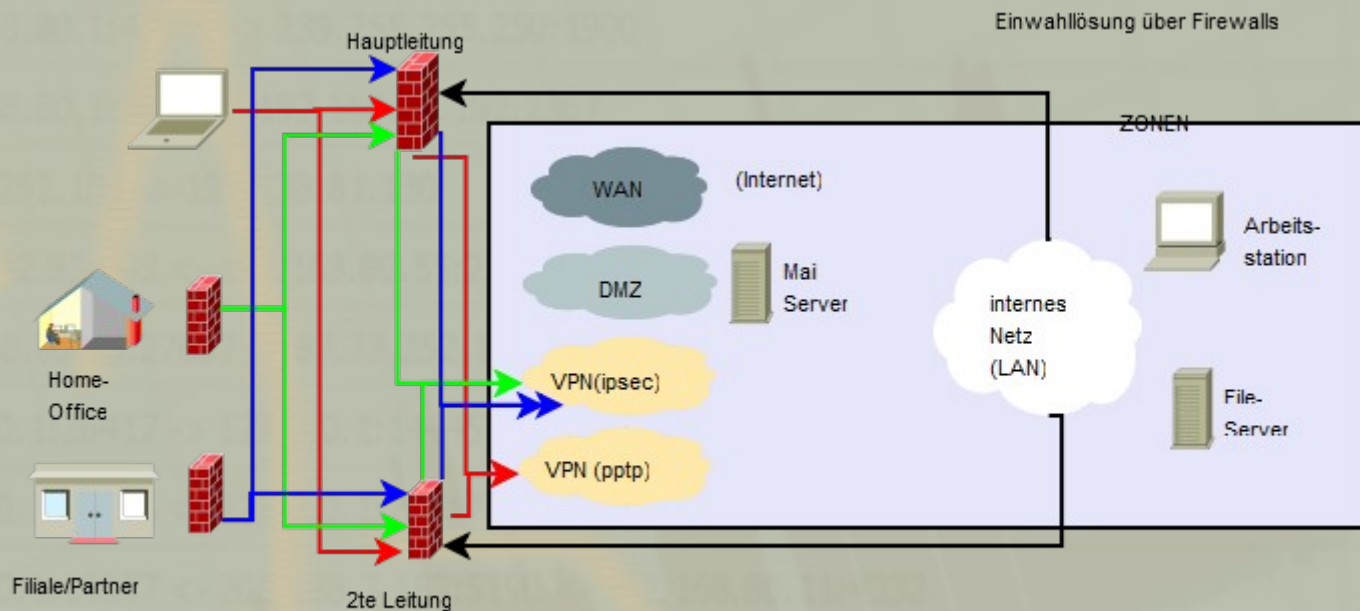
... oder für Firmennetze



(c)2009 C. Marxmeier

...und das auf Basis von **stabiler, stromsparender Hardware** in Verbindung mit **Open Source**..

Beispielaufbau für ein kontrolliertes Firmen-Netzwerk:



(c)2009 C. Marxmeier

Bei dieser Lösung besteht über die 2 Firewalls eine Redundanz für die Einwahl/Erreichbarkeit. Jede logische Zone wird über Regeln in der Firewall kontrolliert.

Die einzelnen logischen Zonen:

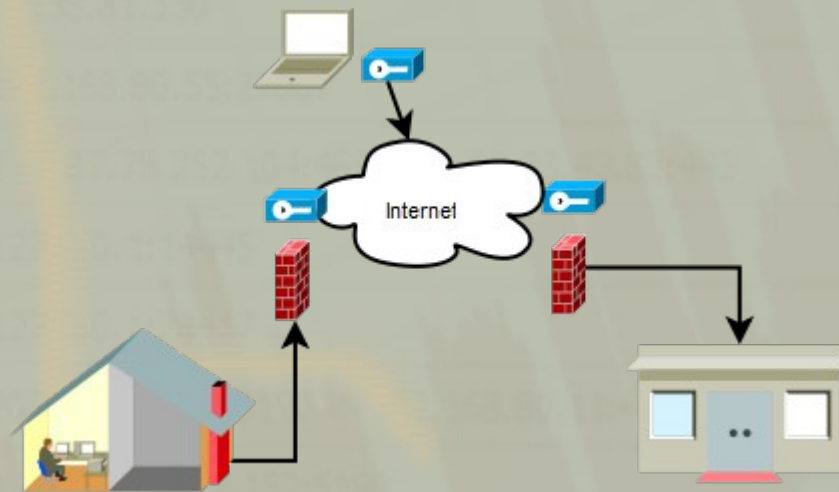
- WAN (Internet)
- LAN (lokales Netz)
- DMZ (s.g. Demilitarisierte Zone, z.B. mit Mailserver)
- VPN (Einwahl von extern)

... laufen physikalisch voneinander getrennt und können über Regelwerke in den Firewalls abgesichert werden.

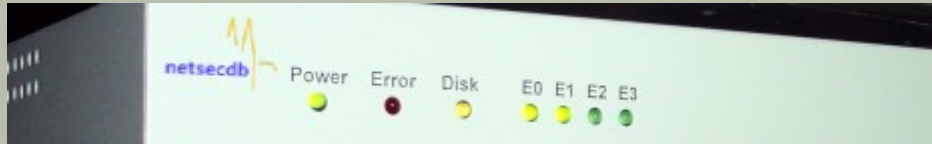
Jeder Zugriff auf Dienste/Daten ist kontrollierbar – Verstöße gegen Sicherheitsrichtlinien nachvollziehbar.

Der Einwahlpunkt für remote-Verbindungen ist die Firewall selbst. Dadurch kann jeder externe Einwahlrechner 'transparent' im Firmennetz abgebildet (so, als ob man ihn lokal anschließen würde), aber seine Zugriffe können gezielt begrenzt werden.

Egal in welcher Umgebung:

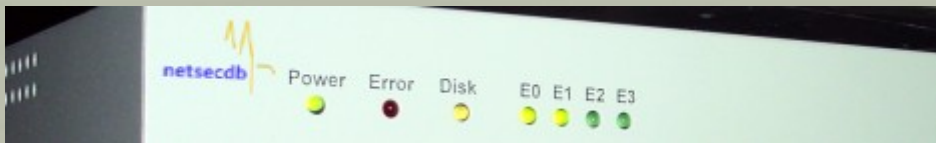


...Verbindungen von unterwegs, dem Home-Office oder aus Filialen erfolgen nur über verschlüsselte Tunnel.

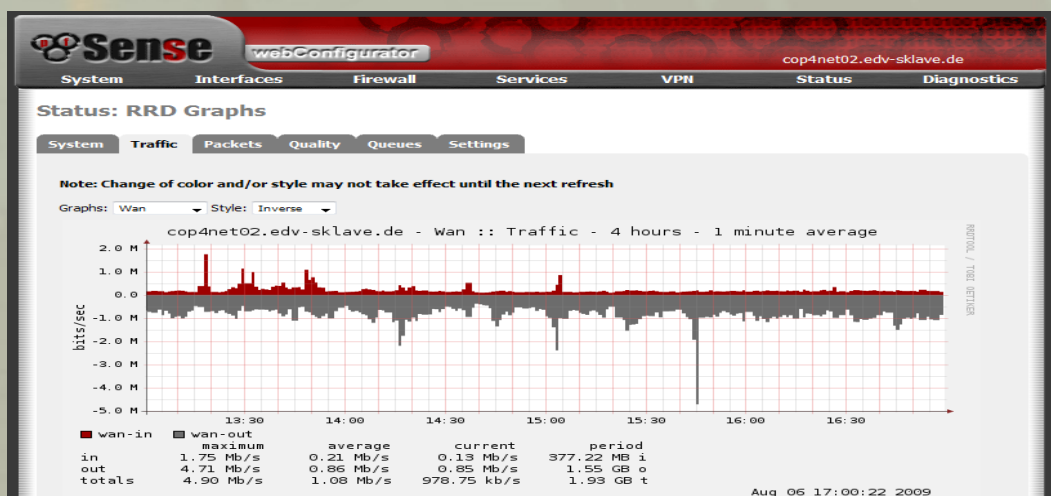


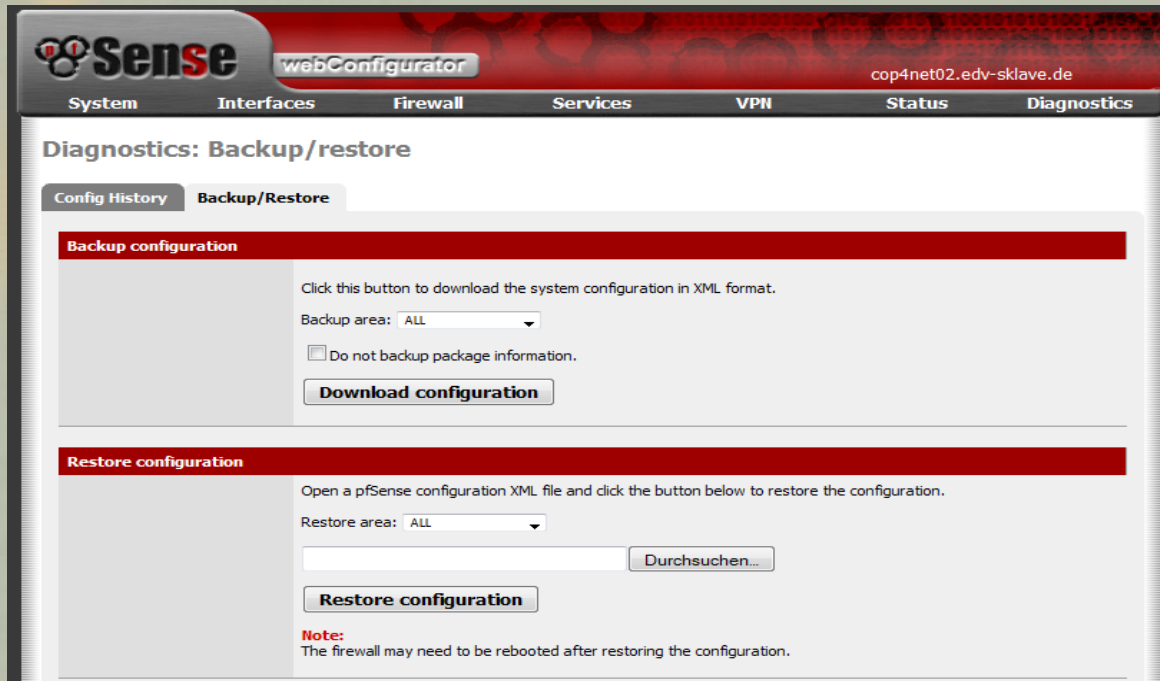
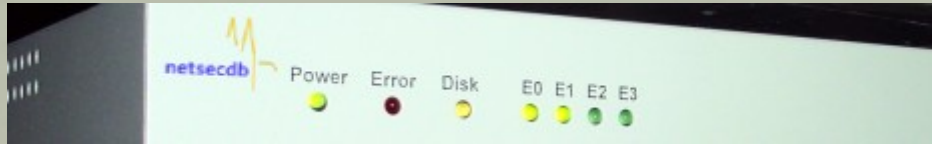
Firewall als Open-Source:






... leicht über ein sicheres Webinterface zu administrieren:





...oder durch das einfache Einspielen eines xml-Files mit gespeicherten Konfigurationsdaten im Klartext – kein verschlüsselter herstellerspezifischer Zeichensalat in der Datei – leicht editierbar.

...ist ja schön – aber wofür soll jetzt die



netsecdb

gut sein?




Ungefähr so durcheinander gewürfelt sieht das Internet für einen Netzwerkadministrator aus.



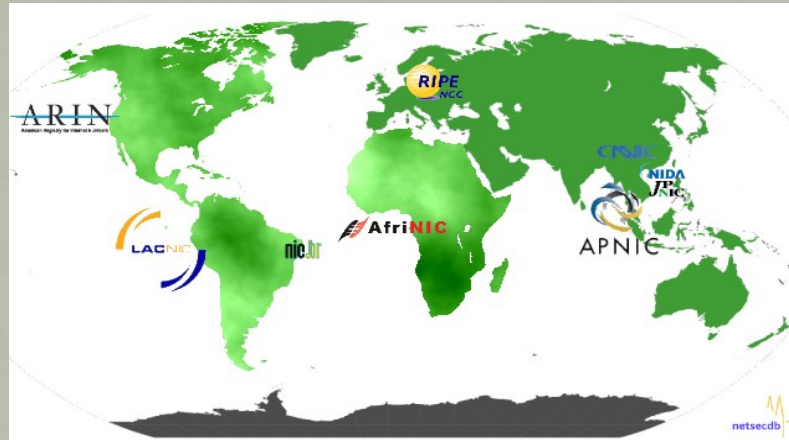
... und etwa so mit Hilfe der

Und wie macht die



netsecdb

das?



Das sind die weltweiten Registries, zuständig für die Vergabe von IP-Adressbereichen:

- ripe, apnic, jpnict, cnic, krnic sind komplett
- arin, lacnic, afrinic, nicbr werden importiert, wenn Daten benötigt werden.

***thanks for their support***

(\*)Die Karte unterliegt der Creative Commons Attribution Lizenz und basiert auf Material von MYGEO Welt.

## Die netsecdb in Stichworten:

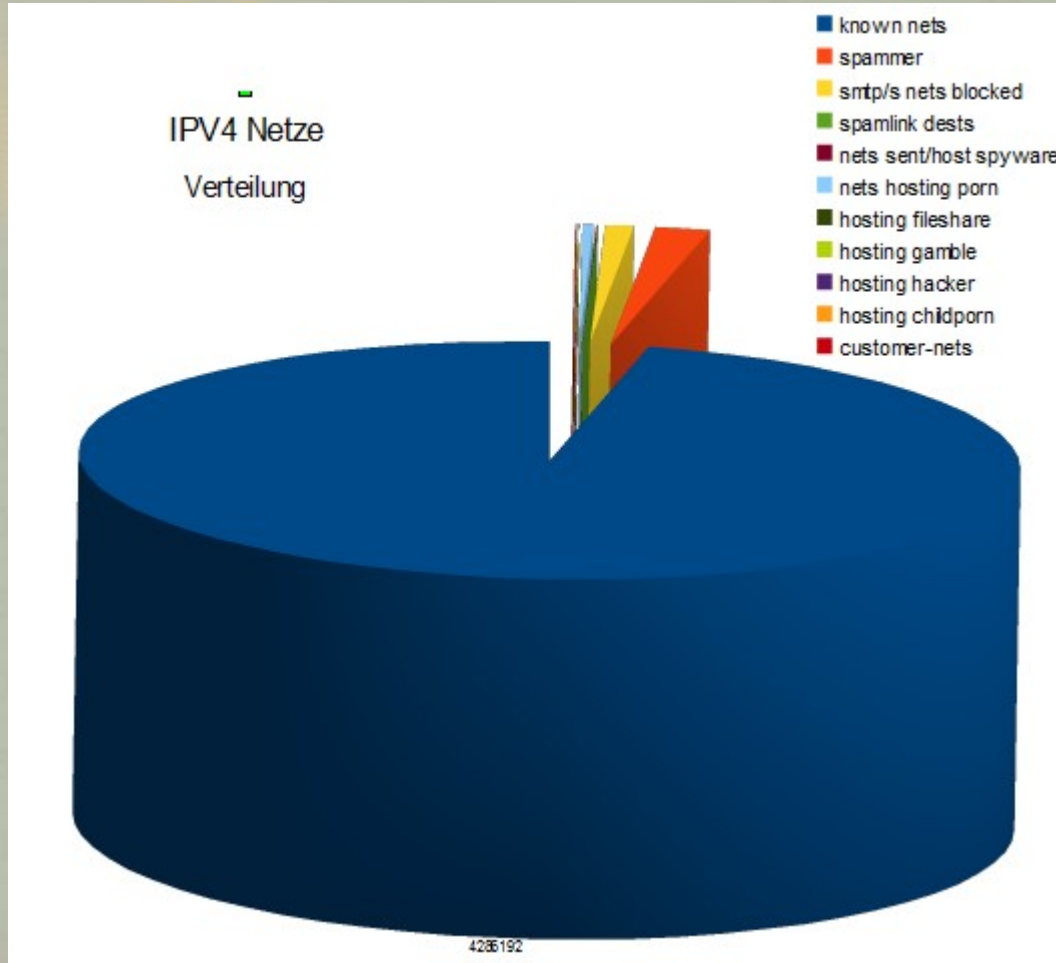


- Wohl größter europäischer, wenn nicht weltweiter Sicherheitsdatenbestand für IPv4-Netze (0.0.0.0-255.255.255.255)
- Stündliche Auswertungsintervalle
- **Lernt selbstständig** aus Logfiles (Firewall, Mail- und Webserver) ständig dazu

## Elektronische "Waffenkammer" zur

- Abwehr
- Filterung
- Analyse (elektronische Rasterfahndung, Beispiel „conficker-Wurm“ mit 2.9 Mio Domains) von Cybercrime aufgrund strukturierter Daten.

Visuelle Auswertung, in welchem Verhältnis die 'missbräuchliche' Nutzung zum bekannten Bestand an registrierten IPv4 Netzen steht.





## Anwendungsgebiete

- Mail-/Web-Server (verschiedenste Standardumgebungen)
- Automatisierte Firewall-Regeln für Linux, Windows und Mac
- Autoupdate über das Internet
- Keine Live-Abfragen wie bei RBL (z.B. ix.manutu = externer Dienst, der bei Anfrage des Mailservers gemeldete Spammer auf IP-Basis zurückmeldet)
- dienstleisterunabhängiges Weiterlaufen auf letztem Config-Stand
- unverschlüsselte Daten (Kunde kann frei anpassen und automatisieren)

## Router/Firewalls

- Datenschutz
- Eindringen verhindern
- sichere Verbindungen schaffen
- Last reduzieren
- Kontrolle

## Home/Office:



- Schutz vor Eindringen/Missbrauch
- Inhaltsfilterung (Stichwort kindersicheres Netzwerk, Cybercrime unterbinden, sichere Zugriffskontrolle)
- Kontrollfunktion (welche Verbindungen von wo nach wo und Inhalt)

## Arbeitsstationen



- Übernahme/Anpassung der Sicherheitslayer für mobiles Arbeiten:
- Konfigurations-templates für Zone Alarm Pro/Suite
- automatisierte Firewall-Konfigurationen für Windows Firewall/Adv. Firewall(nur Vista und größer)

# Produkte für



# Standardumgebungen

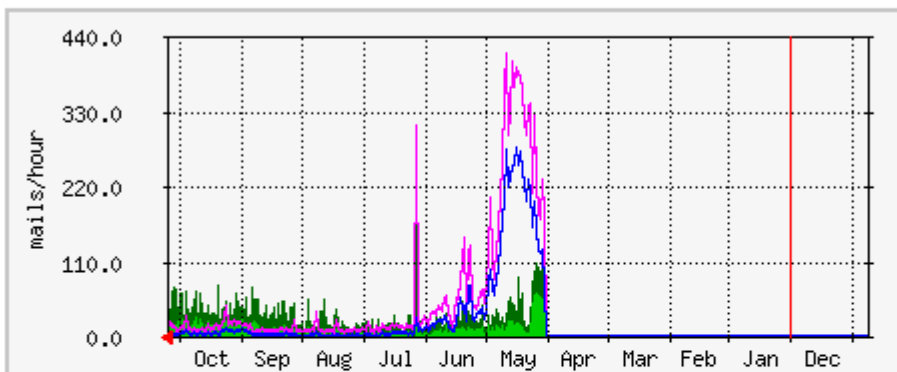


# Anwendungsergebnisse Server 1:

(Zeitachse von rechts nach links)



'Yearly' Graph (1 Day Average)



	Max	Average	Current
<b>CLEAN:</b>	178.0 mails (1.8%)	12.0 mails (0.1%)	23.0 mails (0.2%)
<b>SPAM:</b>	411.0 mails (4.1%)	33.0 mails (0.3%)	4.0 mails (0.0%)

- GREEN ###** clean MAILS
- BLUE ###** rejected SPAM
- DARK GREEN ###**
- MAGENTA ###**

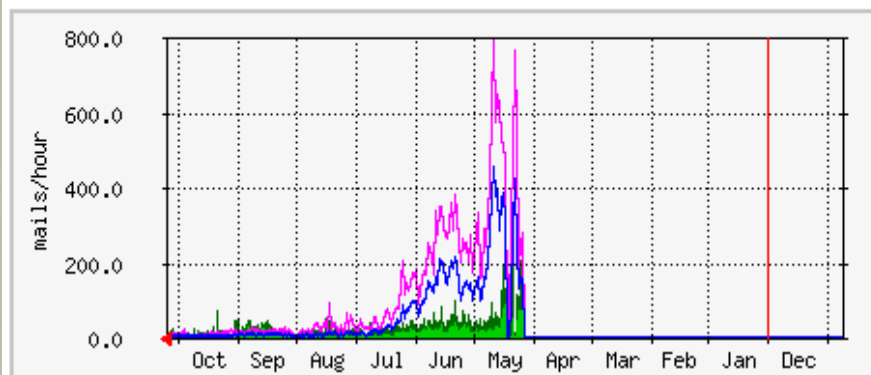
Man kann deutlich die Reduktion des Traffics von 98% im Bereich SMTP sehen und hat damit kaum SPAM's !

# Anwendungsergebnisse Server 2:

(Zeitachse von rechts nach links)



'Yearly' Graph (1 Day Average)



Max **CLEAN**: 226.0 mails (2.3%) Average **CLEAN**: 14.0 mails (0.1%) Current **CLEAN**: 7.0 mails (0.1%)  
Max **SPAM**: 788.0 mails (7.9%) Average **SPAM**: 63.0 mails (0.6%) Current **SPAM**: 2.0 mails (0.0%)

- GREEN ###** clean MAILS
- BLUE ###** rejected SPAM
- DARK GREEN###**
- MAGENTA###**

Man kann deutlich die Reduktion des Traffics von 98% im Bereich SMTP sehen und hat damit kaum SPAM's !

Wir hoffen, die Themen  
nachvollziehbar veranschaulicht  
zu haben.

Falls nicht,  
geben Sie uns bitte ein Feed-Back,  
damit wir diese Präsentation verbessern können.

[info@netsecdb.de](mailto:info@netsecdb.de)

# Danke für Ihre Aufmerksamkeit!



Weitere Infos im Netz unter:

[www.marxmeier.de](http://www.marxmeier.de)  
[www.rettesichwerkann.de](http://www.rettesichwerkann.de)  
[www.netsecdb.de](http://www.netsecdb.de)