DIPLOMARBEIT

"Redesign of a multifunctional, security compliant and highly available Internet access"

TABLE OF CONTENTS

1. Introduction
2. Customer-specific requirements to the environment
3. Analysis of the current situation (problem description)
4. Concept of the future structure (solution)
5. Proof of concept (practrical part)
6. Conclusion
7. Appendix (technical explanations)

NEW CONCEPT

LOADBALANCERS

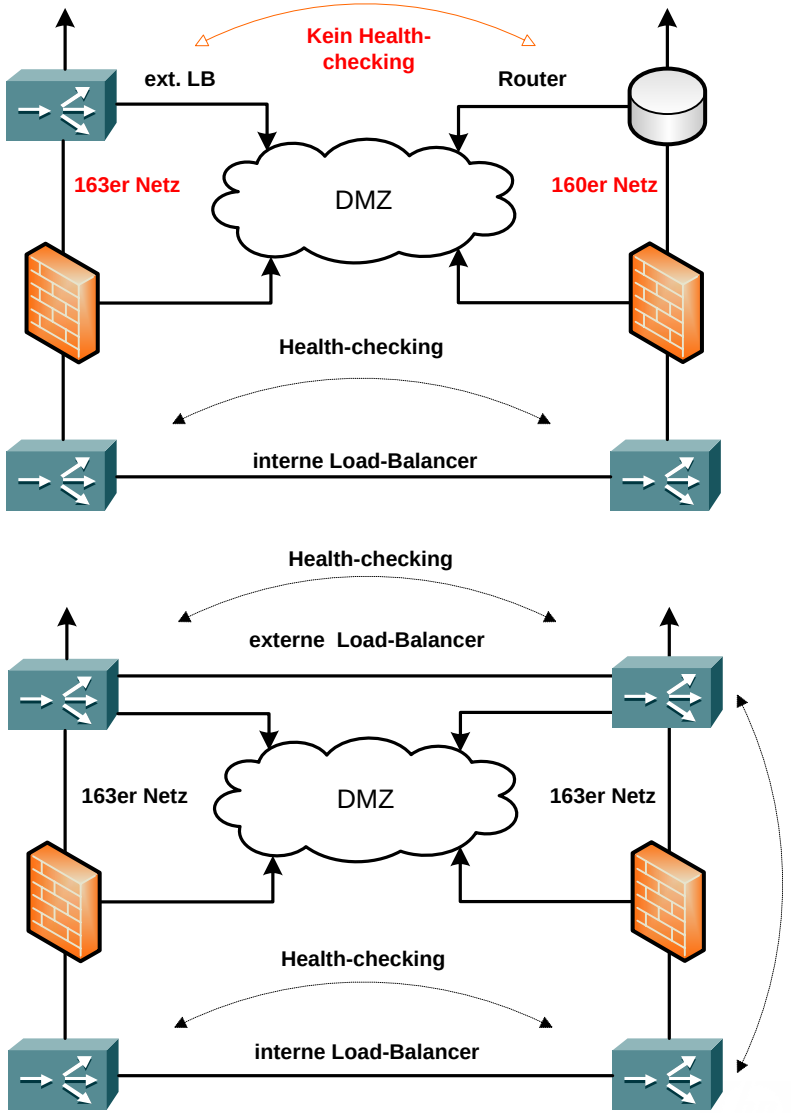
LOADBALANCERS

Ist-Zustand

- keine vollständige Redundanz zum Internet vorhanden
- kein Health-checking im externen Netzwerk zw. Router und LB
- interne LBs out-of-support

Notwendige Maßnahmen um Best Practice zu erreichen

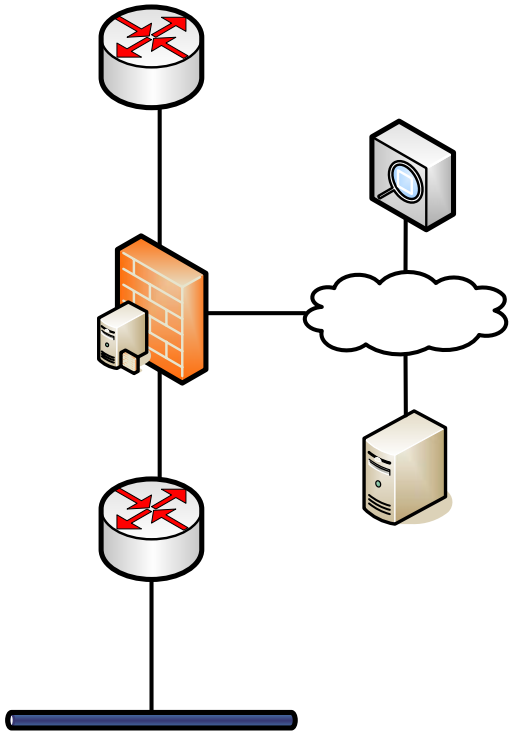
- externe Router zur Verbesserung der Redundanz durch LB ersetzen
- interne LBs durch akt. Geräte mit neuem Supportvertrag ersetzen
- Anmietung einer zusätzlichen Leitung zw. den Rechenzentren
- Anpassung der LB-Konfiguration



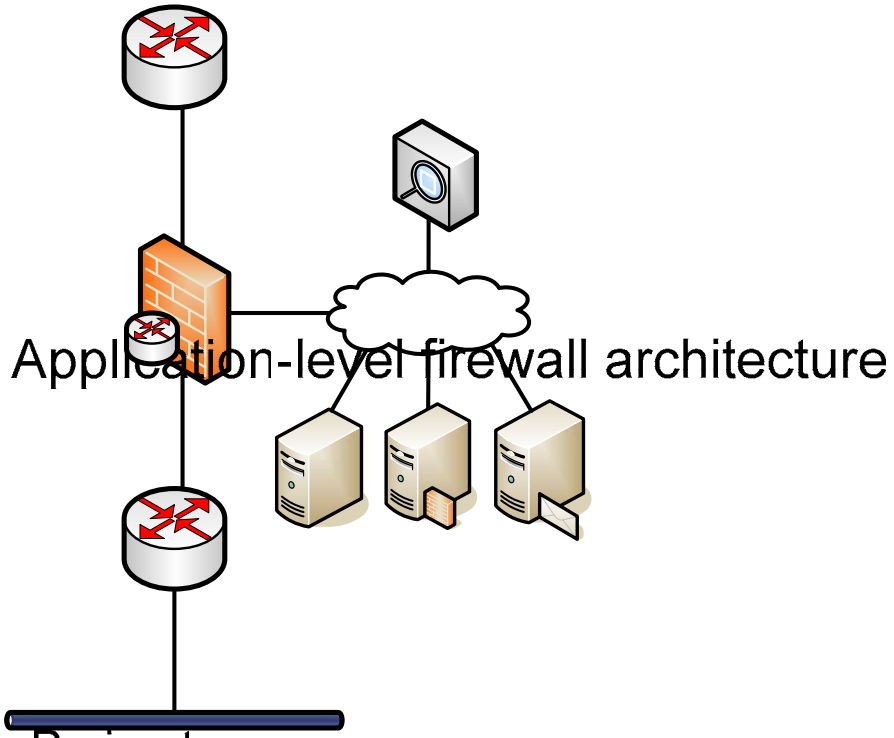
PROXY SERVERS

3-LAYER SECURITY ARCHITECTURE

2 Möglichkeiten zur Implementierung:



aktuell:
non-Cisco architecture (L7-FW)



geplant:
Cisco architecture (L3/4-FW)

IDS

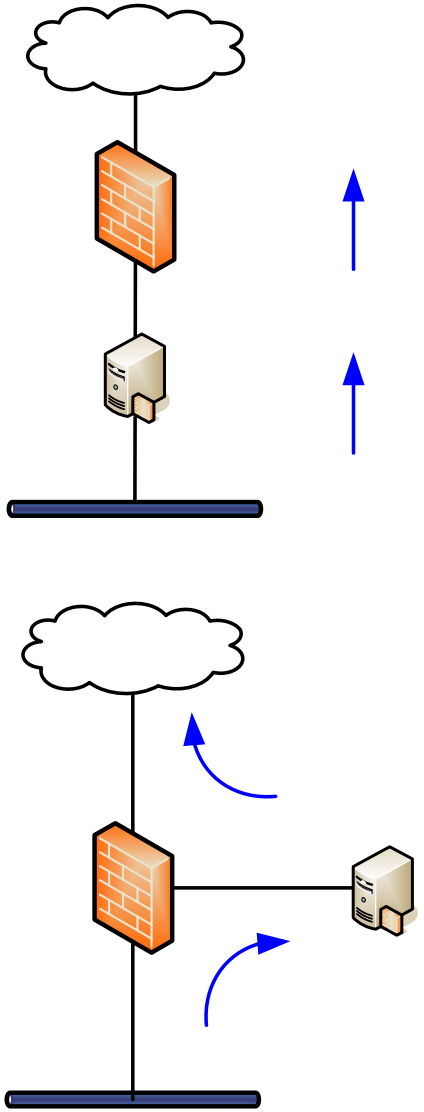
PROXY SERVERS (1)

Ist-Zustand

- Sidewinder-Firewall blockt Webseiten und Applikationen, die nicht RFC-konform programmiert sind
- Absenken des FW-Securitylevels wegen Sicherheitsanforderungen nicht möglich
- nicht-RFC-konformer Traffic wird momentan durch Work-arounds realisiert, keine „Def. Inspection“ → Security Policies !?

Notwendige Maßnahmen

- Umzug der Proxy-Server in eigene DMZ
- Abschaltung der FW „Defense Inspection“ um Kompatibilität zu erhöhen
- Proxy Server übernehmen Packet Inspection auf Applikationsebene (L7)
- Einzelabnahme der Internet-Applikationen



PROXY SERVERS (2)

Vorteile

- Applikationen laufen problemlos
- Vermeidung von Work-arounds
- geringerer Aufwand bei der Implementierung von neuen Anwendungen

Nachteile

- Anpassung der Infrastruktur stellt einen erheblichen Aufwand dar (Zeit & Kosten)
- Routing und Natting muss angepasst werden; Firewalls müssen umkonfiguriert werden
- höhere Firewall-Utilization
- kein IP address logging mehr möglich; Authentisierung dann nur noch mit NTLM

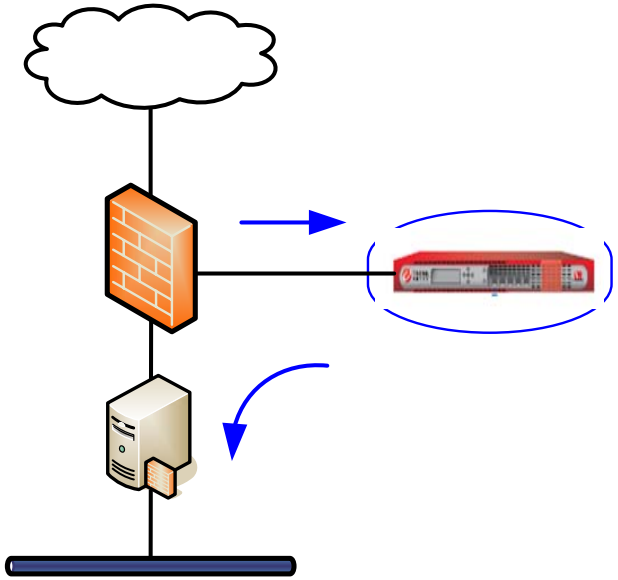
ALTERNATIVE: AV-SCANNER ALS PROXY

Alternative: AV-SCANNER

Warum?

- momentan nur ein (!) Protection Layer
  für allgemeines Virus-Scanning (Clients)

  vgl. dazu Mail-Traffic: drei Protection Layers
  (IronPorts, Notes Mail-GWs und Clients)
- Gefahren aus dem Web nehmen zu*,
  z.B. Malicious Code in ActiveX, Java,
  Downloads, etc.



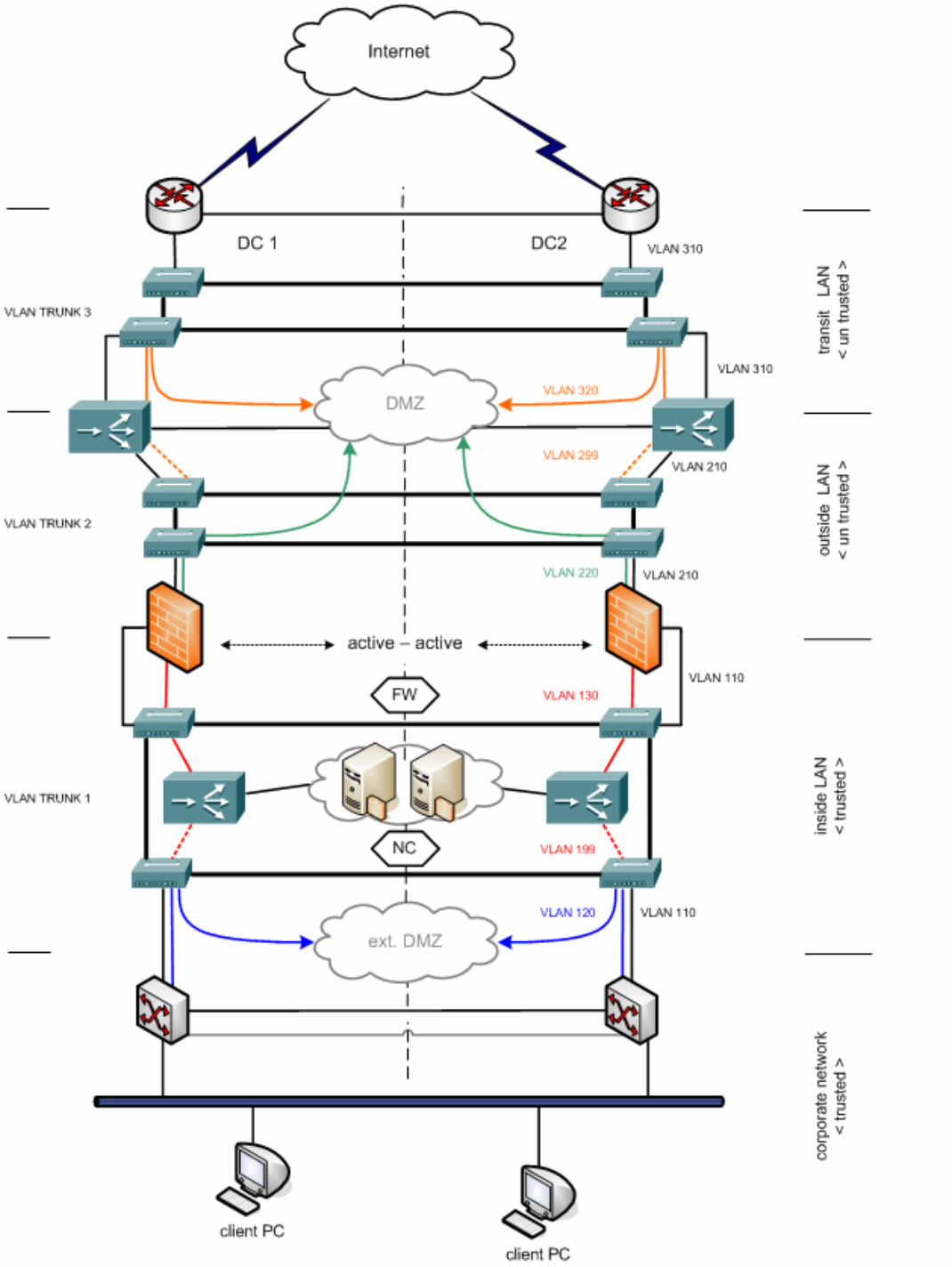
Vorteile

- erhöhte Sicherheit
  - da schon im Netzwerk gescannt wird
  - da zwei versch. Engines benutzt werden
    (einzelne AVs erkennen nie 100%)
- AV-Appliance steht als Proxy in der DMZ,
  NetCache-Umzug evtl. nicht mehr notwendig
- Sidewinders können durch Network-FWs
  ersetzt werden, evtl. Trade-in mit CP oder Cisco

* TM threat trend 2006

LAST BUT NOT LEAST: “GRÜNE WIESE”

New Design


Internet
DC 1
DC2
VLAN 310
VLAN TRUNK 3
transit LAN
< un trusted >
VLAN 310
DMZ
VLAN 320
VLAN 299
VLAN 210
outside LAN
< un trusted >
VLAN TRUNK 2
VLAN 220
VLAN 210
active – active
VLAN 110
FW
VLAN 130
VLAN TRUNK 1
inside LAN
< trusted >
NC
VLAN 199
VLAN 120
VLAN 110
ext. DMZ
corporate network
< trusted >
client PC
client PC


invent