

Freitag, 03.03.2006
IT Security Day
IT Security Day



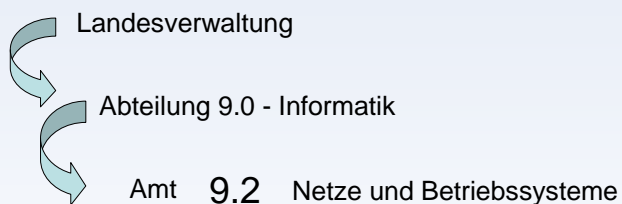
Cisco PIX Firewall: ein guter Chef kann delegieren

Marco Tienghi – Autonome Provinz Bozen



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Das Amt 9.2



Datennetze, Server und Clients (Betriebssysteme)



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Die Arbeit, die Leute



Amt für Netze u. Betriebssystemen – Bereich Netze

Marco Tienghi
Antonella Melchiori
Matteo Cuzzolin
Paolo Realdon
Gianfranco Idini
Hugo Schrott

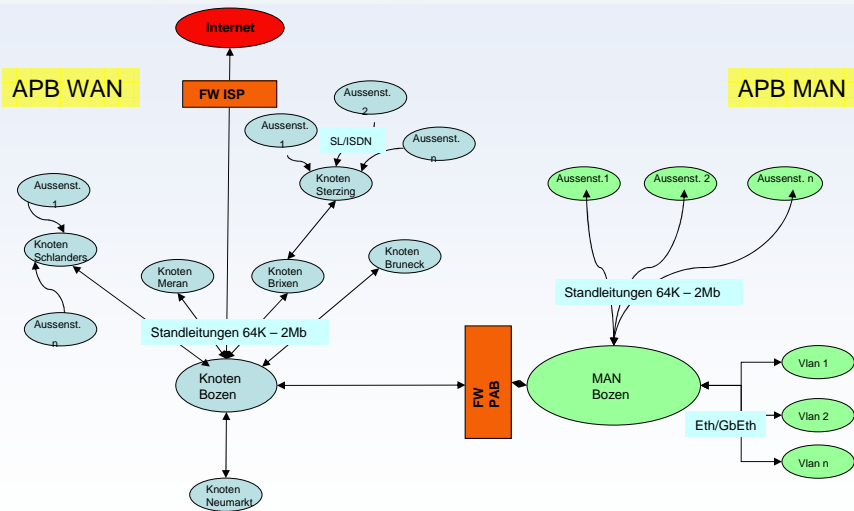
Planung, Realisierung und Instandhaltung von Netzwerken

- Lokale Netze – Stadtnetze – WAN-Verbindungen
- ~ 5000 User
- Technische Räume (~30)
- Aktive NW-Geräte (~150 blöcke)
- Verwaltung Zugänge (Internet-Telearbeit-mobile users)
- Sicherheit im weitesten Sinn



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Das Netz



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi



Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?**
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



Zum Thema



~~Das vorgeschlagene Thema:~~

~~- Cisco-Firewall: Funktionsweise, z.B. Arbeitsweise des Content
Filterings anhand einer Demonstration vorzeigen~~

Leider kein Thema !



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Zum Thema



"Schutz vor Hackern und Spionen"

1: Cisco Firewall kann sehr feinen Analysen auf ISO/OSI level 2→7 machen.

Content filtering ist aber etwas anderes

2: Content-filtering != URL-filtering

User dependent settings → need for authentication and big config effort

Cisco Firewall "gibt es in Outsourcing"



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi



Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann**
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



Physikalischen Eigenschaften

- mechanical robustness
- no moving parts inside (no HDD → Flash FS)
- rack mountable chassis

No OS components to maintain

Many HW sizes – single OS image



Eigenschaften 2



•Release 6.3.5 (Pix 501 → Pix 535)

- Stateful Firewall with Rich Application / Protocol Inspection
- Integrated VPN and In-Line Intrusion Detection
- Market-leading Voice /Multimedia Security
- Cost-Effective High Availability Solution
- Easy-to-use Web-based Management Interface
- Robust Remote Management Options
- Certifications
- Embedded IDS
- And much More

Packet captures



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Eigenschaften 3



Release 7.x (Pix 515 → ASA 5540)

Major PIX 7.0 Enhancements

- ❖ Failover
- ❖ Virtual Firewall
- ❖ Transparent Firewall
- ❖ Modular Policy Framework
- ❖ Quality of Service
- ❖ Application Inspection Engines
- ❖ IP Multicast
- ❖ GTP
- ❖ IPv6
- ❖ Remote Access VPN
- ❖ S2S VPN
- ❖ Extensibility
- ❖ Other Enhancements



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Application Inspection & Control Engines



- Provide Control over Application Usage & Network Access
- Application and protocol-aware inspection services provides strong application-layer security
- Performs conformance checking, state tracking, security checks, NAT/PAT support and dynamic port allocation

Multimedia / Voice over IP

H.323 v1-4
SIP
SCCP (Skinny)
GTP (3G Wireless)
MGCP
RTSP
TAPI / JTAPI



Core Internet Protocols

HTTP
FTP
TFTP
SMTP / ESMTP
DNS / EDNS
ICMP
TCP
UDP

Database / OS Services

ILS / LDAP
Oracle / SQL*Net (V1/V2)
Microsoft Networking
NFS
RSH
SunRPC / NIS+
X Windows (XDMCP)

Specific Applications

Microsoft Windows Messenger
Microsoft NetMeeting
Real Player
Cisco IP Phones
Cisco Softphones

Security Services

IKE
IPSec
PPTP

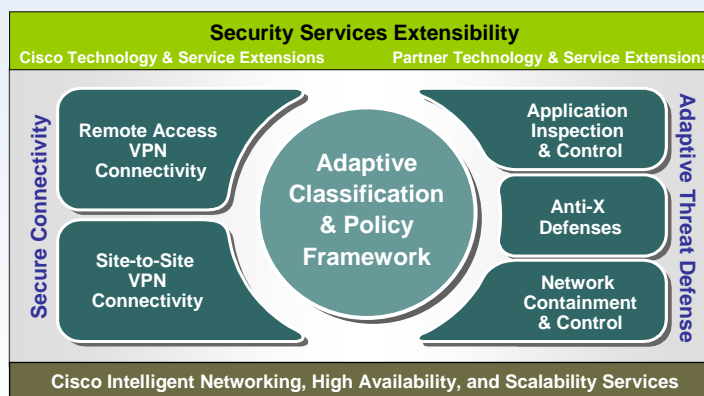


PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Adaptive Identification and Mitigation (AIM) Srv. Architecture



Technology Extensibility to Mitigate Current and Future Threats



Innovative AIM services architecture allows business to adapt and extend the security services profile via Cisco-developed and partner-provide innovations delivering high current services performance and services extensibility



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Wunschliste



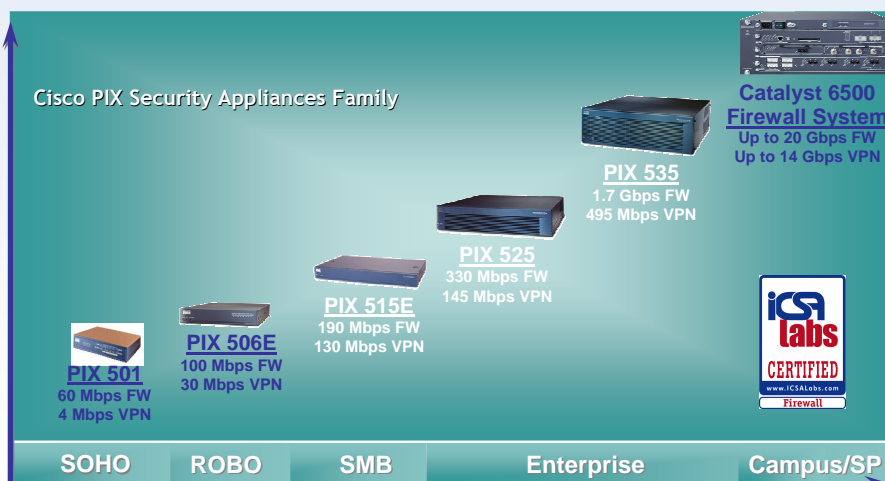
Unerfüllte Wünsche

- Internes logging (nur Buffer logging verfügbar)
- Schnellere GUI
- WAN interface types (es gibt aber **IOS Firewall !!!**)



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Cisco PIX Series Product Lineup



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Cisco ASA 5500 Feature Overview






- 🔒 Adaptive Identification and Mitigation (AIM) Services Architecture
- 🔒 Adaptive Threat Defense Capabilities
 - Application Security
 - Anti-X Defenses
 - Containment and Control
- 🔒 Secure Connectivity Capabilities
 - Remote Access Connectivity
 - Site-to-Site Connectivity
- 🔒 Converged Security and VPN Management
- 🔒 Hardware Features and Performance Metrics



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Cisco ASA 5500 Series Product Lineup



	Cisco ASA 5510 	Cisco ASA 5520 	Cisco ASA 5540 
Target Market	SMB and SME	Enterprise	Large Enterprise
List Price	Starting at \$3,495	Starting at \$7,995	Starting at \$16,995
Performance Max Firewall Max Threat Mitig. (FW+IPS) Max IPSec VPN	300 Mbps 150 Mbps 170 Mbps	450 Mbps 375 Mbps 225 Mbps	650 Mbps 450 Mbps 325 Mbps
Base Platform Services	App FW, IPSec and SSL VPN, and more A/S HA (Upg.), 3 FE to 5 FE	Same as 5510, plus A/A Failover, VPN Clustering, 4 GE + 1 FE	Same as 5520, with higher performance and scalability



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi



Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann

-warum eine Kommerzielle Lösung?

- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



- Leistungen
- Failover: stateful, active/active
- Virtual firewall (security contexts) – transparent mode
- VPN failover
- Clustering
- Fein Konfigurierbar
- Support
- Zentrale Verwaltung
- Events correlation
- Einheitliche Programmier-UI
- ...



User Interface - → v6.x



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Virtualized Services and Transparent Operation

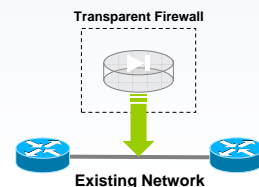
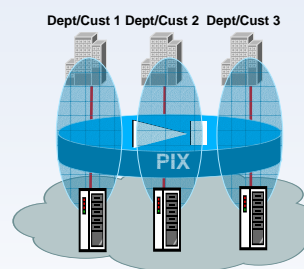


Scalable Security Services

- Adds support for Security Contexts (virtual firewalls) to lower operational costs
 - Enables device consolidation and segmentation
 - Supports separated policies and administration

Easy to Deploy Firewall Services

- Introduces transparent firewall capabilities for rapid deployment of security
 - Drops into existing networks without need for readdressing the network
 - Simplifies deployments of internal firewalling and security zoning - new applications

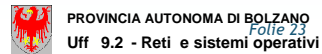
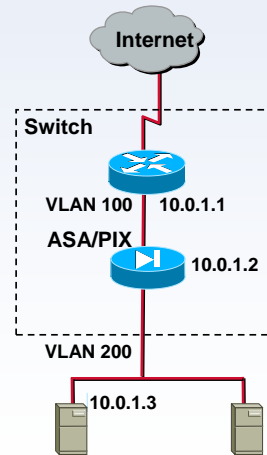


PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Transparent Firewall



- The transparent PIX/ASA uses an inside interface and an outside interface only.
- Each directly connected network must be on the same subnet.
- A management IP address is required for each context, even if you do not intend to use Telnet to the context.
- For multiple context mode, each context can use the same (overlapping) subnet or different subnets under different Vlan, sharing of VLAN not allowed
- Dynamic routing protocols will not run on the device. However it can be pass through.
- NAT is not supported.
- You can also optionally use an EtherType ACL to allow non-IP traffic through.



Converged Mgmt, Monitoring & Response



Device Management

- Integrated, web-based mgmt
- Converged configuration – FW, IPS, VPN, AV
- Real-time monitoring tools

Cisco Adaptive Security Device Manager (ASDM)

System Management

- Multi-device integrated mgmt
- Enterprise-scale provisioning

CiscoWorks VPN/Security Management (VMS) System
Solsoft Policy Server

Monitoring and Mitigation

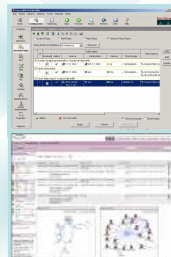
- Multi-platform event management and response
- Sophisticated data reduction and correlation

Cisco Security MARS
CiscoWorks SIMS

Auditing

- Device posture validation against industry “best practices” and regulatory compliance

Cisco Security Auditor





Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?

-Websense und SmartFilter (N2H2)

- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



- 2 Officially Cisco supported integrations
- Am anfang nur URL filtering
- Nicht im Box integriert – verlangt externes Server
- FW ↔ Server Dialog mittels eigenes Protokoll
- Internen Listen ↔ Abonnement an Listen klassifizierter Sites
- Websense ist am meistens bekannt
- SmartFilter (ehem. N2H2) – eine Version ist besonders für Schulen gemeint

- www.websense.com
- www.securecomputing.com



Websense integration

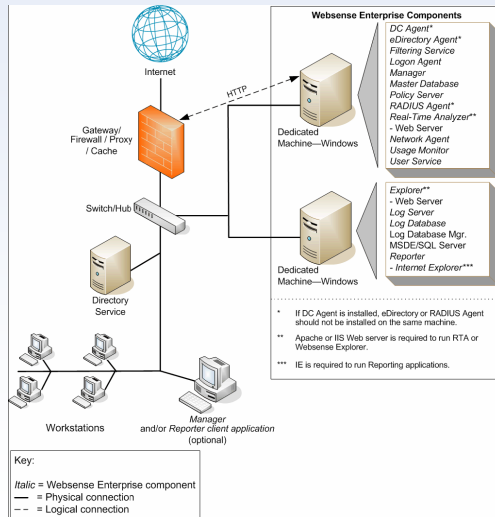
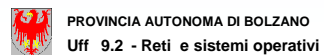


Figure 1 Synopsis of Windows Deployment in a Small Network



SmartFilter integration

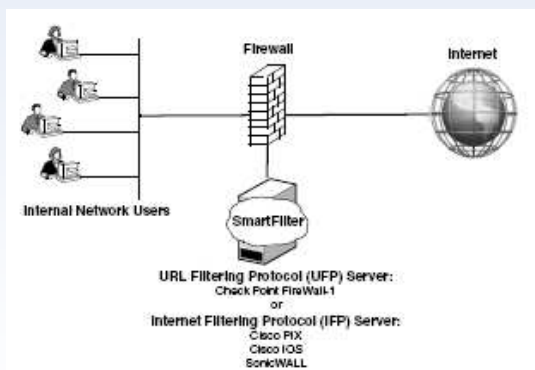


Figure 1 Synopsis of Windows Deployment in a Small Network



URL Filtering 2



**Eigentlich geht es meistens nicht um Content filtering
sondern um URL filtering**

**Es wird nicht das Inhalt gecheckt,
sondern seine externe Form (wie es erscheint)
oder sogar nur das Behälter**



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

URL Filtering 3



- Es gibt Systemen, die URL Filtering ziemlich gut machen können, auch ohne zusätzlichen Anwendungen
- Oft braucht man kaum Downloadable Categorized Sites Lists, sondern nur intern erstellten White/Black Lists
- Man muss die Endbenutzer unterscheiden Können und entsprechend Sites sperren oder nicht
- Logging (und Privacy Bestimmungen – Aufbewahren der Logfiles?)
- unerwünschten Nebenwirkungen (internen Links werden blockiert, CC Tickets geöffnet, u.s.w.)



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Verteilung der Arbeit 1



Eine alternative Lösung:

- Firewall soll Firewall spielen
- Internet Surfen am FW gesperrt außer...
- ...für Content Filtering Gerät

Vorteile:

- ermöglicht getrennte Verwaltung.
- Netzwerk Mgr muss nicht Polizeirolle auf sich nehmen



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Verteilung der Arbeit 2



Welchen Gerät ?

- MS ISA-Server 2004
- Squid
- SurfControl
- ...

Für Kleinbetriebe auch: Privoxy, FreeProxy, ...



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Zum Inhalt

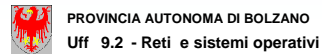


Cisco Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)

-andere Möglichkeiten

- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



Alternativen



PROPRIETARY

- Cisco ASA
- Cisco NAC
- CheckPoint Firewall-1
- Juniper
- Fortinet Fortigate (ASIC)
- Secure Computing Sidewinder
- Crossbeam
- NetApp NetCache
- MS ISA-Server based appliances

OPEN SOURCE (and derivatives)

- Monowall
- IP-Cop (Endian Firewall)
- Smoothwall
- Squid based appliances
- Privoxy
- FreeProxy
- Linux / BSD tailored systems
- und Firewall Builder




Alternativen



m0n0wall webGUI Configuration

System information

Name	m0n0wall.neon1.net
Version	1.2 built on Sun Oct 9 18:58:23 CEST 2005
Platform	wrap
Uptime	00:34
Last config change	Mon Oct 10 10:59:55 CEST 2005
CPU usage	view graph
Memory usage	 36%

m0n0wall

- <http://m0n0.ch/wall/>
- No HD required
- CFG on floppy / USB key
- Small size
- Runs on Old PC's



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Alternativen



```
root@Devil:~# netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
Active UNIX domain sockets (servers and established)
Proto RefCnt Flags   Type       State          I-Node Path
unix  3      [ ]     DGRAM     3142           /dev/log
unix  2      [ ]     DGRAM     3230
root@Devil:~# ps ax
PID TTY      STAT   TIME COMMAND
  1 ?        S      0:05  init [3]
  2 ?        SW     0:00  [keventd]
  0 ?        SWM    0:00  [ksoftirqd_CPU0]
  0 ?        SW     0:00  [kswapd]
  0 ?        SW     0:00  [bdflush]
  0 ?        SW     0:00  [kupdated]
 10 ?        SW     0:00  [khubd]
106 ?        S      0:00  /sbin/devfsd /dev
121 ?        SW     0:00  [kpmd]
404 ?        S      0:00  syslog-ng
407 ?        S      0:00  klogd -c 2
623 uc/1     S      0:00  -bash
624 uc/2     S      0:00  /sbin/agetty tty2 9600
625 uc/3     S      0:00  /sbin/agetty tty3 9600
626 uc/4     S      0:00  /sbin/agetty tty4 9600
627 uc/5     S      0:00  /sbin/agetty tty5 9600
628 uc/6     S      0:00  /sbin/agetty tty6 9600
629 uc/8     S      0:00  /bin/procinfo -f -F /dev/tty8
631 uc/1     R      0:00  ps ax
root@Devil:~#
```

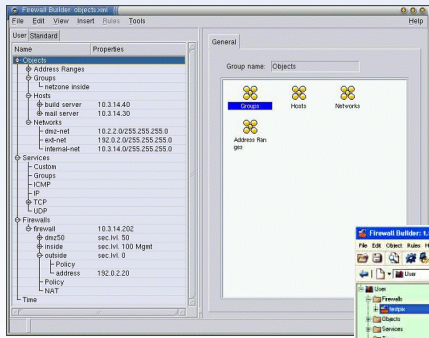
Devil Linux

- <http://www.devil-linux.org/>
- No HD required
- CFG on floppy / USB key
- 170MB
- No GUI
- Runs on Old PC's (486)
- supported by FW Builder



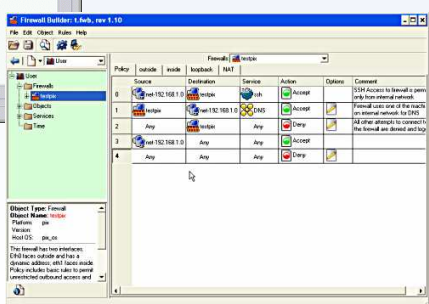
PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Alternativen



Firewall Builder

- www.fwbuilder.org
- FW configuration utility
- Multiple FW support
- Runs on Linux and Win



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Anderen Möglichkeiten



Cisco PIX Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten .

-case study: Autonome Provinz Bozen

-neuen Trends ---> neue Geräte



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Case study



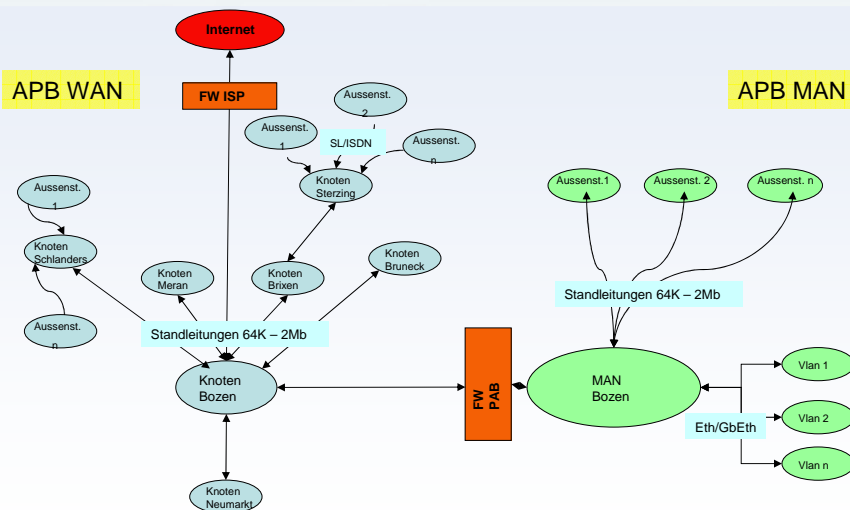
- 10 Cisco Pix firewall verschiedener Größen
- Filter network trafic
- Site 2 site VPN
- Mobile user VPN

- Kontrollierten Internetzugriff für ~ 5000 Benutzer
- 80 LAN Landesweit + Schulen
- ~ 150 komplexe Netzgeräte zu verwalten



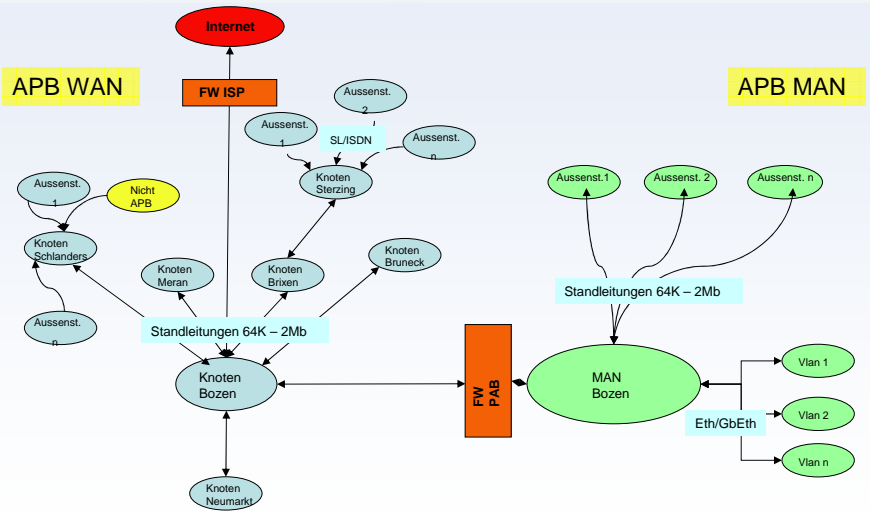
PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Das Netz



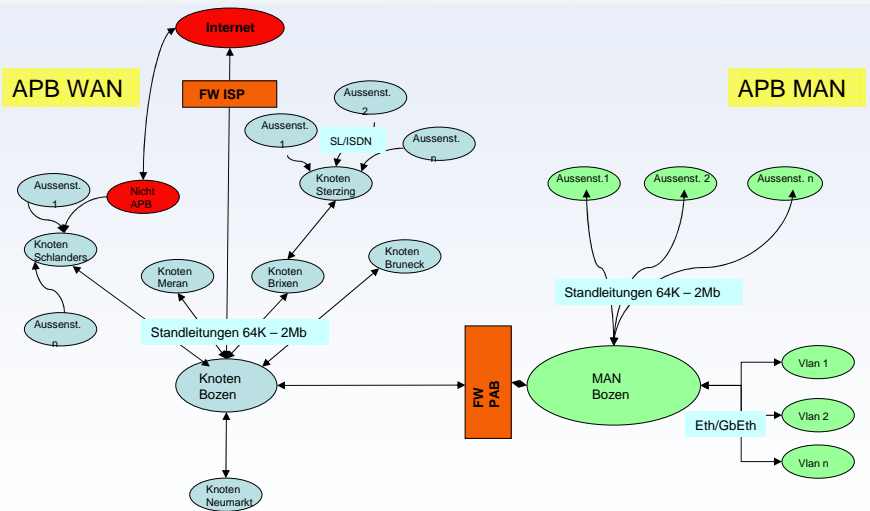
PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Das Netz



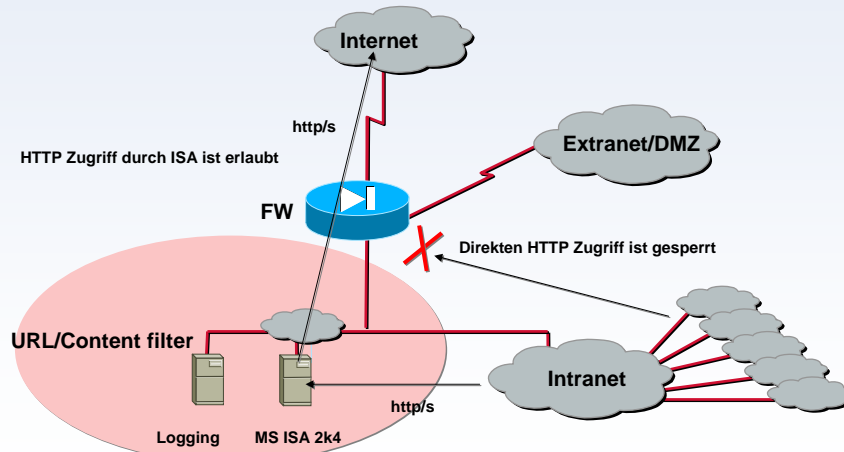
PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Das Netz



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Case study



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Case study



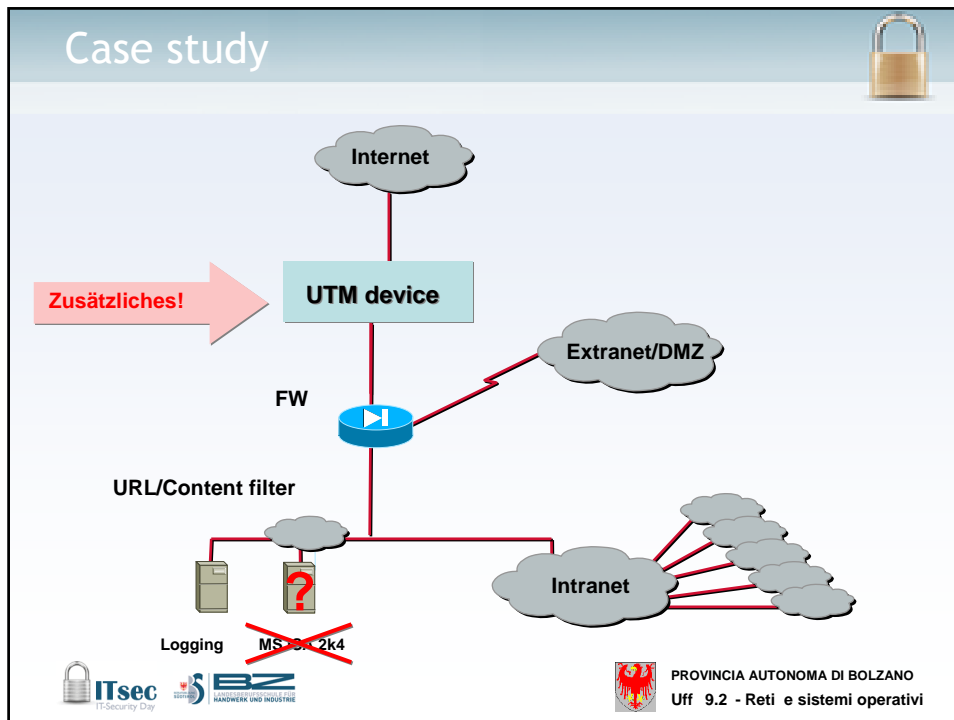
Offenen Problemen:

- ISA Stabilität
- Konfigurationen speichern/History
- Verwaltung
- OS Patches
- Redundanz ???



PROVINCIA AUTONOMA DI BOLZANO
Uff. 9.2 - Reti e sistemi operativi

Case study

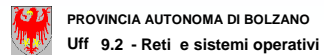


Zum Inhalt



Cisco PIX Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ----> neue Geräte**



Neuen Trends



ASIC based Geräte

Firewall und filtering Engine in Hardware

UTM (Unified Threat Management)

Ein Gerät für alles: Firewall, URL/Content Filtering, Antivirus, Antispam

NAC (Network Admission Control) o.ä.

Netzwerkzugang wird verwaltet – End Device soll Policies unterstehen

SSL VPN

Clientless personalized and secured communications



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Alternativen



PROPRIETARY

- Cisco ASA
- Cisco NAC
- CheckPoint Firewall-1
- Juniper
- Fortinet Fortigate (ASIC)
- Secure Computing Sidewinder
- Crossbeam
- NetApp NetCache
- MS ISA-Server based appliances

OPEN (and derivates)

- Monowall
- IP-Cop (Endian Firewall)
- Squid based appliances
- Linux / BSD tailored system



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Zum Inhalt



Cisco PIX Firewall: ein guter Chef kann delegieren

- woher einen solchen Titel?
- was Cisco Firewall selber (nicht) kann
- warum eine Kommerzielle lösung?
- Websense und SmartFilter (N2H2)
- andere Möglichkeiten
- case study: Autonome Provinz Bozen
- neuen Trends ---> neue Geräte



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi

Zum Schluss



DANKE für Ihre Aufmerksamkeit

- Fragen ?
- Demo-Area

marco.tienghi@provinz.bz.it



PROVINCIA AUTONOMA DI BOLZANO
Uff 9.2 - Reti e sistemi operativi