

Netzwerk-Segmentierung und -Sicherheit

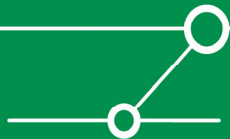
Enno Rey, erey@ernw.de
CISSP, CISA



ERNW



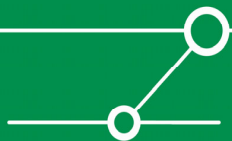
- Gegründet Sommer 2001 durch Enno Rey
- Netzwerk-Dienstleister mit Sicherheits-Fokus
- Aktuell zehn Mitarbeiter
- Schwerpunkte: Security Management, Audit/Revision, Security Research, Penetrations-Tests
- Kunden: Industrie, Banken, Behörden, Provider



Agenda



- Zweck und Nutzen von Netzwerk-Segmentierung
- Ansätze der Segmentierung
- Sicherheits-Aspekte und typische Fehler
- Segmentierung mit VLANs
- Sicherheitsprobleme durch Cisco DTP und VTP



Wozu Segmentierung?

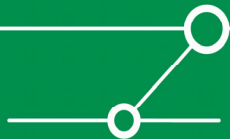


„Alte Welt“

- Schützenswert sind einige wenige Systeme (e.g. Server)
- Vergleichsweise statische Netze m. wenigen Aus-/Übergängen
- Flache Netze mit Security Devices „nach aussen“ (Firewalls)

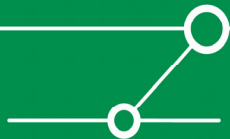
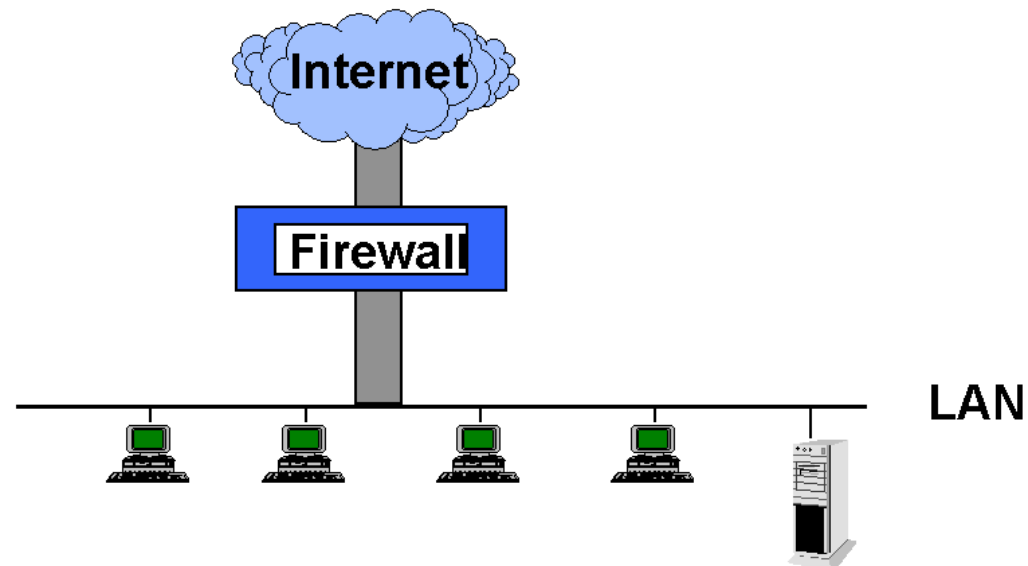
Heutige Realität

- Schützenswert sind (fast) alle Systeme (vor allem auch Clients)
- Dynamische Netze mit vielen Übergängen und mobilen Geräten
- Sicherheit „im Netz“ erforderlich



Das klassische Firewall-Modell

entnommen aus einem Foliensatz von 1997



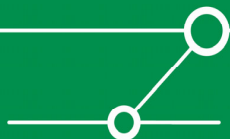
Das klassische Firewall-Modell



- Noch immer entspricht dies in etwa dem in vielen Organisationen anzutreffendem Design.
- Die hier symbolisierte 'Firewall' kann dabei durchaus aus mehreren Einzelkomponenten bestehen (inkl. AV-Gateway, Content Filter etc.).

Zentrale Konzepte sind hier:

- **Perimeter Defense/Border Defense:** Gefahren-Abwehr an der Netzwerk-Grenze
- **Choke Point:** der gesamte Netzwerk-Verkehr muss über diese(n) Punkt(e) fließen, um dort geprüft/kontrolliert/geregelt zu werden.

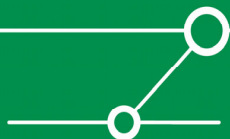


Grundannahmen des klassischen Firewall-Modells



Dieses Design setzt implizit u.a. voraus:

- **Alle internen Hosts sind vertrauenswürdig (*trusted*).**
[vergleiche etwa Architektur der *Cisco PIX*].
- **Alle internen Systeme haben denselben Schutzbedarf.**
- **Es gibt eine klare Grenze zwischen 'innen' und 'außen'.**
- **Gefahren kommen in erster Linie 'von außen'.**
- **Die Firewall kann diese Gefahren erkennen und abwehren.**

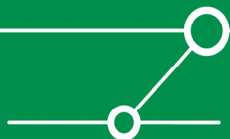


Kritik dieser Grundannahmen



“Alle internen Hosts sind vertrauenswürdig (*trusted*).”

- In den internen Netzen sind zunehmend Geräte, die dort nur temporär sind & die sich oft auch ‘außerhalb’ befinden (Laptops, PDAs, ggf. private PCs).
- Die Systeme werden bedient von Menschen (*Usern*)...
- Die Vertrauenswürdigkeit der Systeme hängt weiterhin von ihrer Konfiguration ab (Patch-Level, Aktualität der Viren-Signaturen, System-Konfiguration etc.).
- Dies alles können die FW-Admins üblicherweise überhaupt nicht einschätzen... weil unterschiedliche Abteilungen für Firewalls & Desktop-Rechner zuständig sind.
- Wer & wo ist ‘intern’?

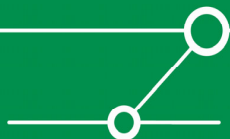


Kritik dieser Grundannahmen



“Es gibt eine klare Grenze zwischen innen und außen.”

- Diese Grenze wird aufgeweicht eben durch Systeme, die nur temporär im internen Netz sind (s.o.).
- Interne Netze werden logisch erweitert durch VPNs... mit ggf. unkontrollierbaren Endpunkten.
- Sie werden möglicherweise auch physisch erweitert durch Wireless-Technologien (WLANs, Bluetooth etc.).
- Es gibt immer mehr ‘Partner-Anbindungen’, Wartungszugänge etc.
Diese sind zwar durchaus ‘kontrollierbar’, machen aber die Regelsätze dann unübersichtlicher und damit meist fehlerhaft(er).

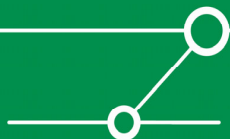


Kritik dieser Grundannahmen



“Gefahren kommen in erster Linie von außen.”

- S.o.: die Systeme werden bedient von Menschen (*Usern*)...
- Gestattet *Ihre* Firewall eingehend Port 135 oder 1433?
Und trotzdem haben sich SQL-Slammer und W32/Blaster in Unternehmensnetzen ausgebreitet...
- Selbst wenn dem so *wäre... könnten* Sicherheits-Probleme ja auch intern entstehen... und damit jenseits der Zuständigkeit einer *Border Defense*-Firewall.

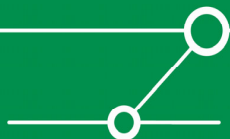


Kritik dieser Grundannahmen



“Die Firewall kann diese Gefahren erkennen und abwehren.”

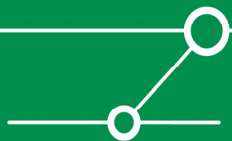
- Firewall-Technologie und –Implementierung hinken der technischen Entwicklung (von Übertragungs-Mechanismen/Protokollen) deutlich hinterher (siehe Instant Messaging, VoIP, SOAP etc.).
- Sicherheits-relevanter Verkehr kann leicht getunnelt werden (insbesondere über HTTP oder auch SSL/TLS).
- Firewalls können nur (stark) beschränkt mit verschlüsseltem Verkehr umgehen.
- Ausblick: Diese Probleme werden mit IPv6 noch größer.



Weitere Probleme



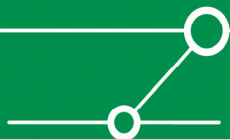
- Eine *Border Defense/Choke Point* Firewall bildet oft einen Flaschenhals für die Kommunikation... und verlockt dadurch, sie zu umgehen.
- Es wird ggf. ein falsches Bewusstsein von Sicherheit erzeugt ("wir haben doch eine Firewall").



Wozu Segmentierung (aus Security-Sicht)?



- Systeme mit unterschiedlichem Schutzbedarf werden voneinander getrennt
- An Übergängen („im Netz“) Security-Enforcement möglich
- Management/Monitoring/Logging werden *gegebenenfalls* vereinfacht, weil idealerweise Systeme mit ähnlichen (Schutz-) Anforderungen in Segmenten zusammengefasst sind
=> damit etwa einheitliches Management möglich.
- Segmentierung kann Probleme adressieren, die aufgrund von Zuständigkeiten/veralteter Technologien/Technologien schwächerer Sicherheit (e.g. WLANs) sonst nicht lösbar sind.
[„Lässt sich ein Security-Problem nicht am (End-)Punkt lösen, stelle ich einfach ein filterndes Device davor.“]



Arten der Segmentierung



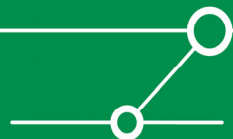
- Statisch/Administrativ, meist für Server
- Dynamisch (etwa anhand von Knoten-Eigenschaften), meist für Clients



Statische/Administrative Segmentierung



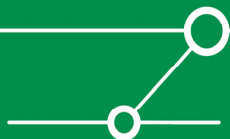
- Es werden Segmente definiert und eingerichtet.
- Systeme werden (nach Risiko-Analyse) in diesen Segmenten platziert.
- Die Segmente sind mit unterschiedlichen „Sicherheits-Regeln“ versehen, etwa hinsichtlich der Konfiguration der Systeme.
- Verkehr zwischen Segmenten wird gefiltert/verschlüsselt/etc.
- Nachfolgend ein Beispiel aus einer deutschen Provider-Umgebung („Zonen-Modell“).



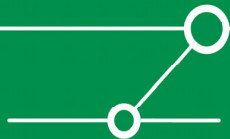
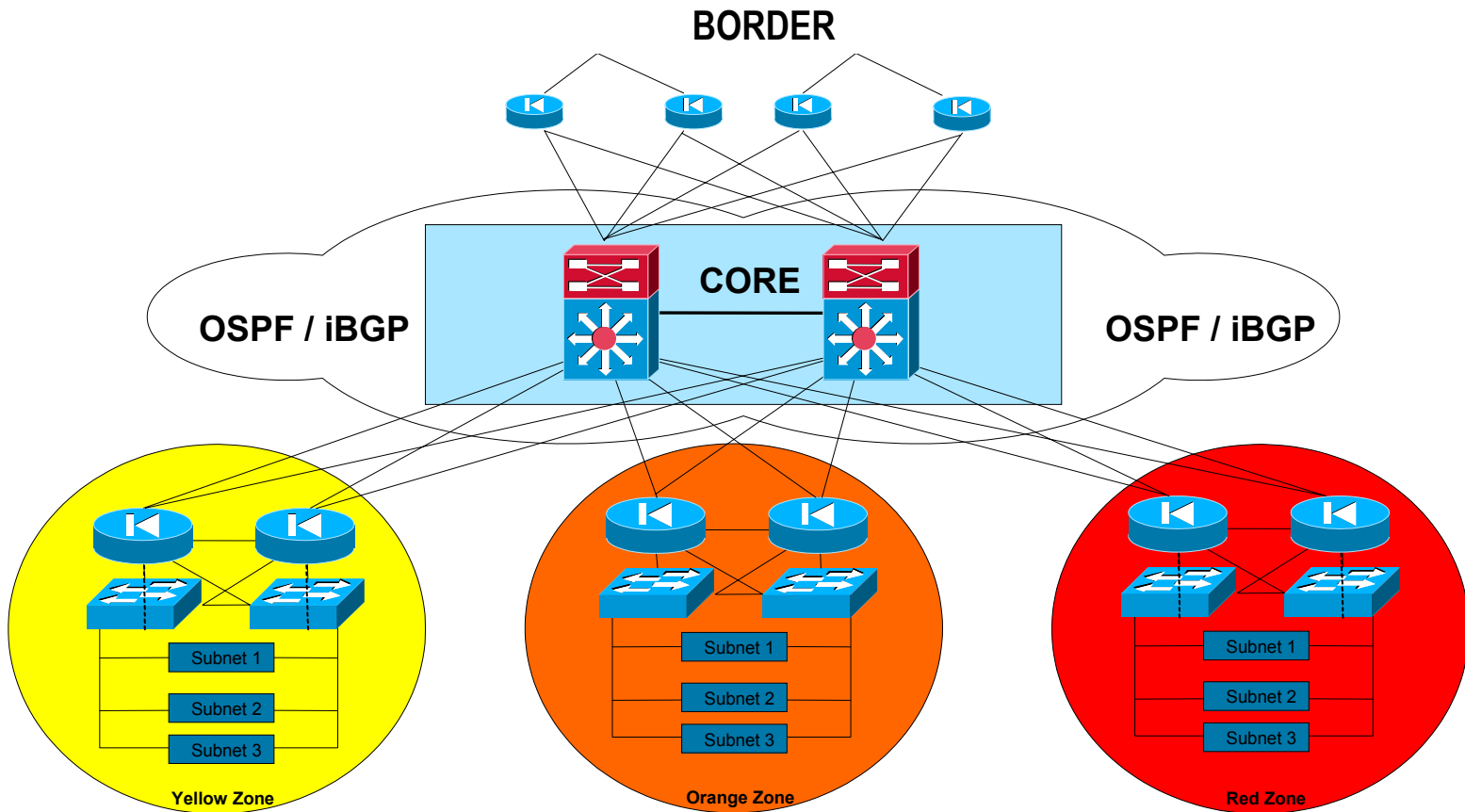
Grundlegendes Konzept



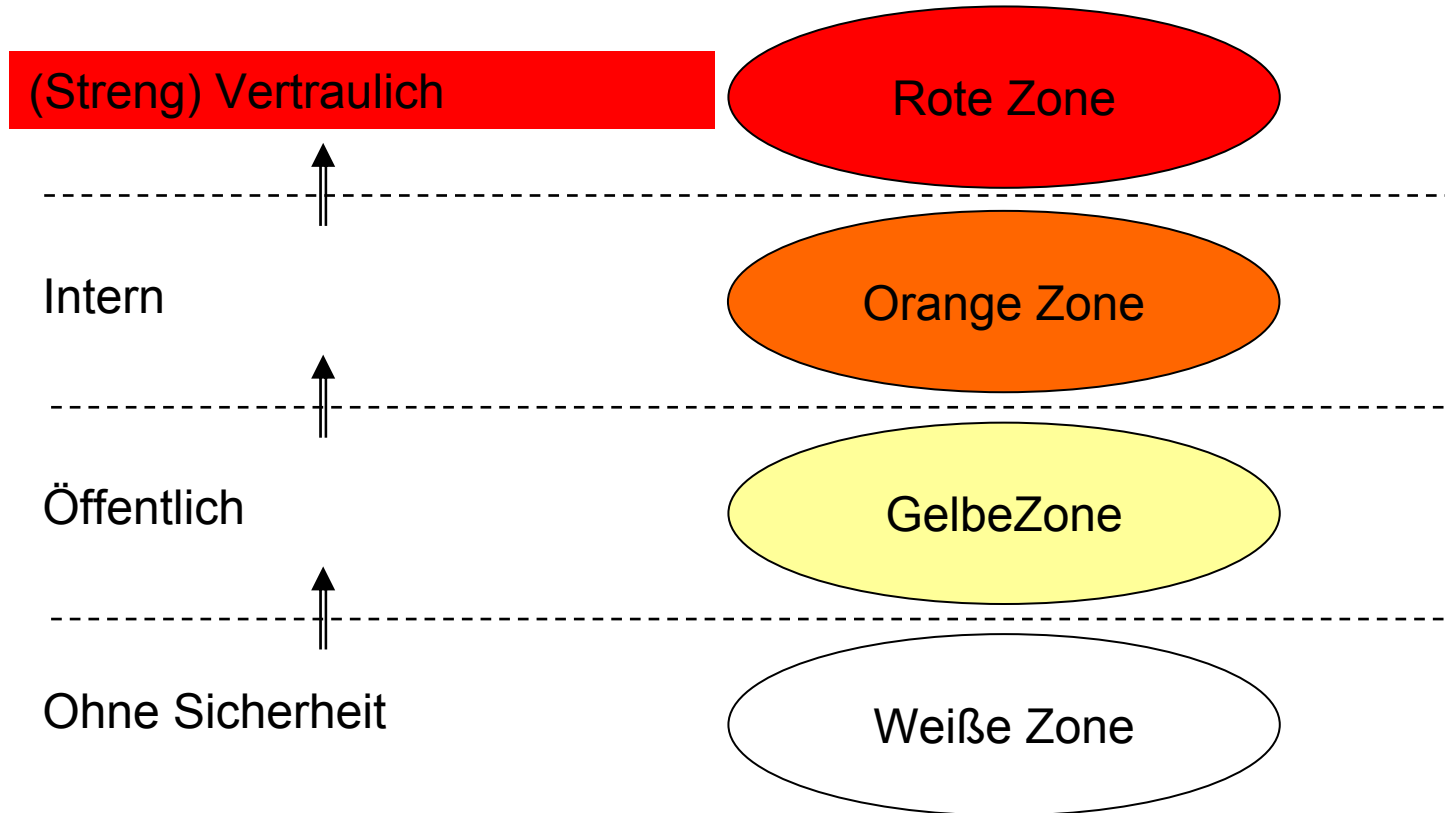
- Das gesamte Netzwerk wird in Segmente (“Zonen”) mit unterschiedlichen Sicherheits-Anforderungen unterteilt. Die Zonen sind physisch voneinander getrennt und können in sich nochmals (etwa anhand von Anwendungen) unterteilt werden (z.B. mit VLANs).
- Alle Netzwerk-Entitäten im weitesten Sinn (etwa Applikationen, Systeme, User) werden durch ihre jeweiligen Owner/Verantwortlichen je einer Zone zugeordnet.
- Pro Zone gelten bestimmte Massnahmen zu Installation/Konfiguration/Betrieb der Systeme (bspw. Richtlinien hinsichtlich Dokumentation, User-Verwaltung, Zugriffsregelung, Hardening, Logging, Business Continuity etc.).
- Die Kommunikationsbeziehungen zwischen den Zonen sind genau geregelt; im Beispiel sind etwa nur Kommunikationsbeziehungen zwischen benachbarten Zonen gestattet und bestimmte Kommunikationsvorgänge müssen zwingend verschlüsselt werden.



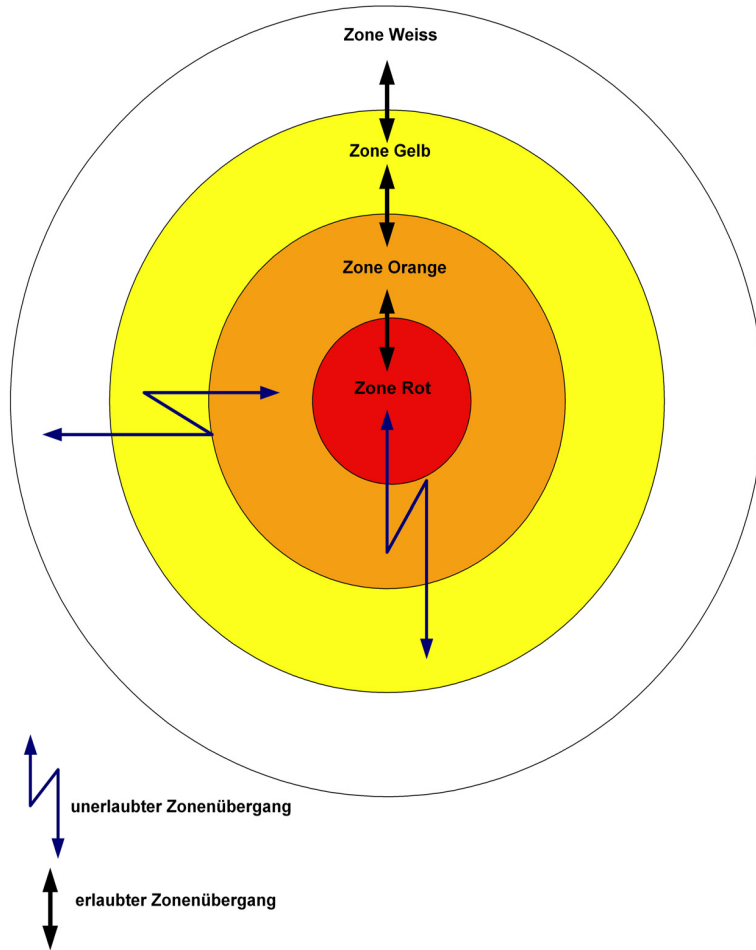
Beispiel zur Netz-Segmentierung



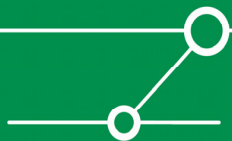
Beispiel zur Netz-Segmentierung



Beispiel zur Netz-Segmentierung, Kommunikationsbeziehungen

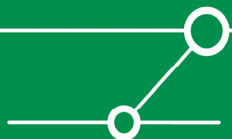


nach Zone / von Zone	Weiß	Gelb	Orange	Rot
Weiß	OK	OK	X	X
Gelb	OK	OK	OK	X
Orange	X	OK	OK	OK
Rot	X	X	OK	OK

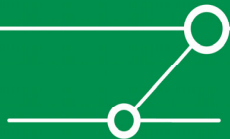
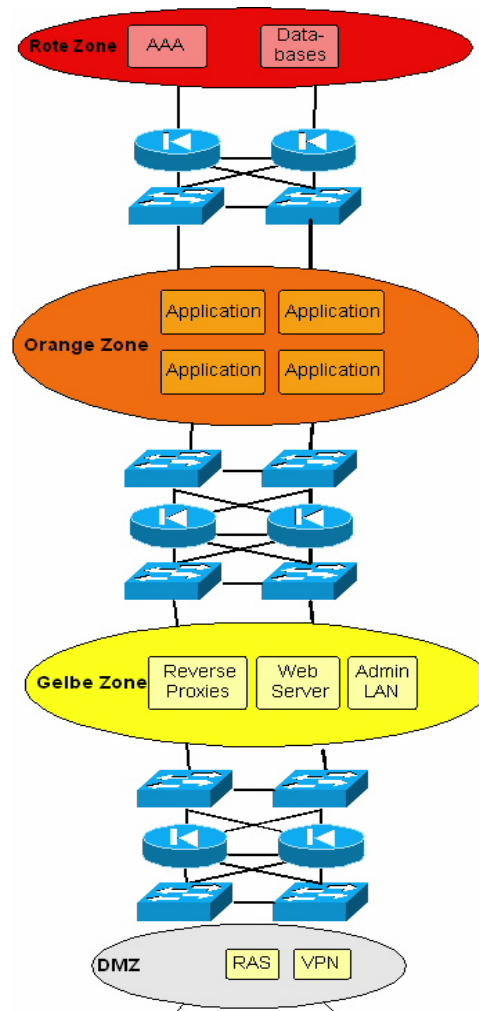


Beispiel zur Netz-Segmentierung, Kommunikationsbeziehungen

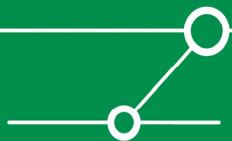
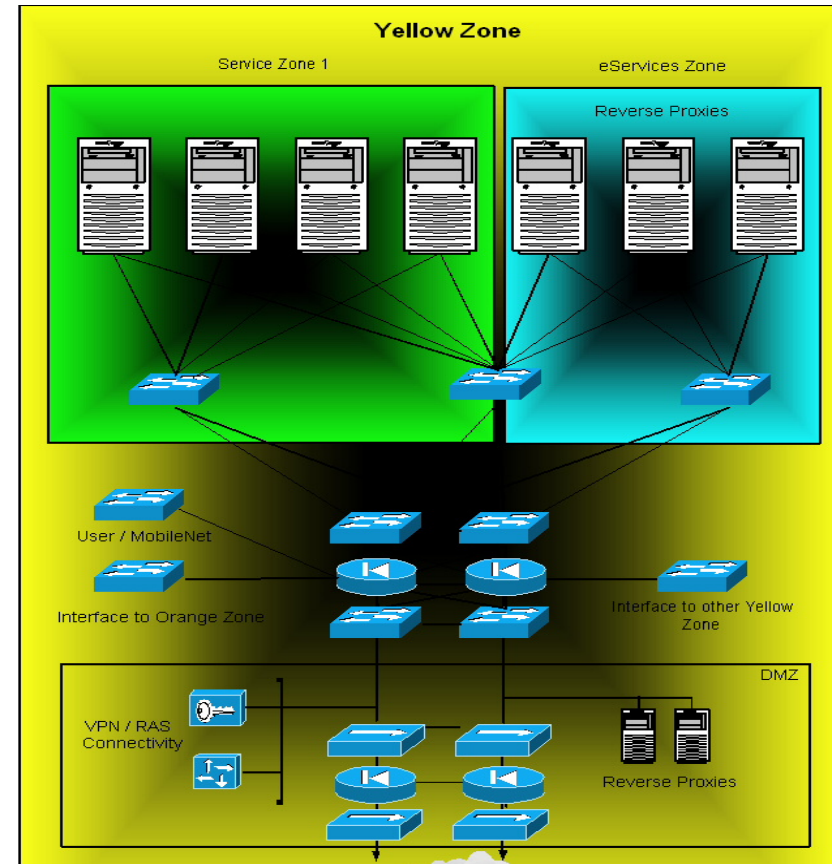
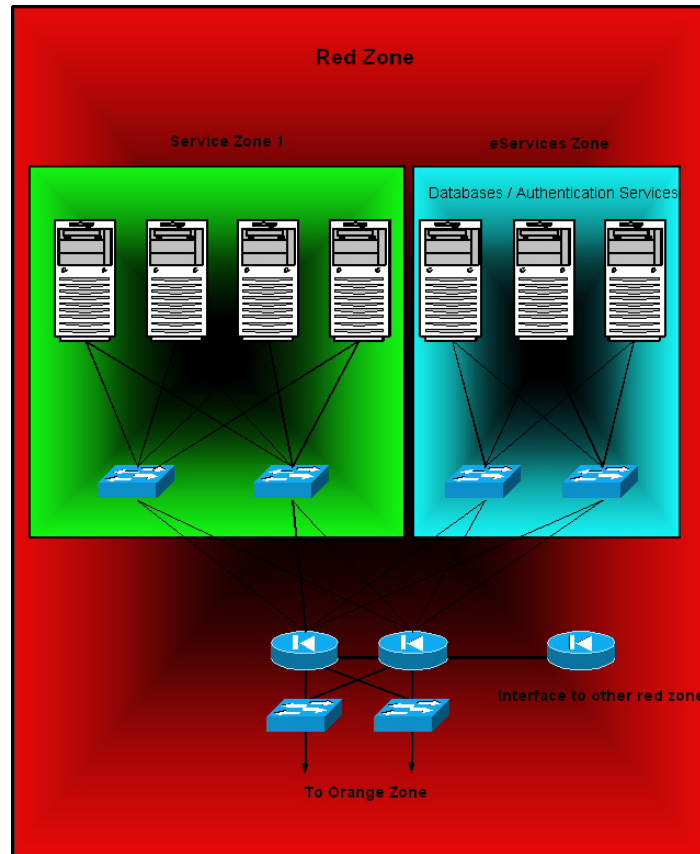
Datenquelle in Zone	Applikation in Zone	Übergang zu Zone	Verschlüsselung
Rot	Orange	Gelb	Ja
Rot	Orange	Orange	Ja
Orange	Orange	Gelb	Ja
Orange	Orange	Orange	Ja
Orange	Gelb	Weiß	Ja
Orange	Gelb	Gelb	Ja
Gelb	Gelb	Weiß	Nein
Gelb	Gelb	Gelb	Nein



Beispiel zur Netz-Segmentierung, Komponenten



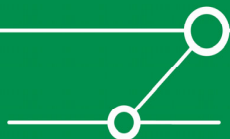
Beispiel zur Netz-Segmentierung, Detail-Ansicht



Statisch/Administrative Segmentierung, Probleme



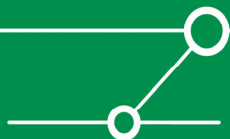
- Das klassische Problem: organisatorischer Soll-Zustand versus ggf. technischer Ist-Zustand.
- Die vorgenommene Zonen-Einstufung bestimmt *anschliessend* ein administratives (menschliches) Handeln, das zu einer bestimmten Systemkonfiguration führen *soll*.
- Platzierung in einem bestimmten Segment bedeutet i.a. auch *Verantwortung*.
- Anzahl der Kategorien/Segmente sollte klein gehalten werden(Anzahl der Ausnahmen auch)
=> meist aufwendige Diskussionen...
- Kann eine sinnvolle Re-Evaluierung beim schnellen Technologie-Wandel in modernen Netzen gewährleistet werden?



Dynamische Segmentierung



- Untersuchung/Bewertung des Security Levels von jedem Knoten
- Segmentierung des Netzes anhand dieses Security Levels
- Anwendung einer Policy auf jedes Netzwerk-Segment
- **Theoretische Erörterung im (nicht mehr gültigen) IETF-Draft *Quarantine Model Overview for IPv6 Network Security [draft-kondo-quarantine-overview-01]. [1]***
- **Produkte etwa:**
Cisco Network Admission Control/Self Defending Networks
Alcatel OmniSwitches mit Automated Quarantine Engine
Microsoft
Check Point *Integrity*
etc.

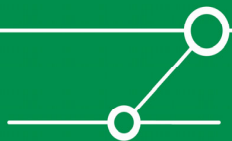


Ermittlung des Security Levels



Zugrundeliegende Parameter können hier etwa sein:

- OS & Software-Versionen
- Installierte Patches
- Installierte Security Software (Anti-Virus, Lokale Firewall etc.)
- Konfiguration & Einstellungen



Segmentierung anhand des SecLevels



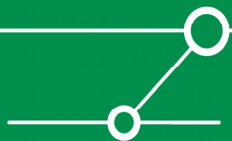
- Die Segmentierung wird durch Netzwerk-Devices vorgenommen.
- Beteiligte Technologien können etwa sein: 802.1x, VMPS, DHCP Option 82 etc.
- Segmentierung wird z.B. gewährleistet durch: VLANs, IP-Subnetze, MPLS u.a.
- Meist ergänzt durch Traffic-Kontrolle zwischen Segmenten



Anwendung von Policies auf Segmente



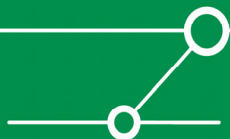
- Bestandteile einer Policy können sein:
Authentifizierungs-Erfordernisse (etwa von Knoten mittels Zertifikaten)
Paketfilter
Routing-Pfade
Bandbreiten-Begrenzungen (Wurm-Traffic!)
usw.



Segmentierung mit VLANs



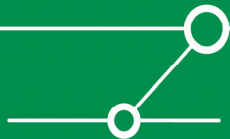
- Typischer Ansatz in vielen Netzen
- Segmente werden mithilfe von VLANs auf einer ‚shared [switch] infrastructure‘ abgebildet
=> Optimierung von HW-Kosten/Support-Verträgen und Admin-Knowhow
- Kommunikation zwischen Segmenten muss geroutet werden
- Und kann dabei gefiltert werden, bei Einsatz von L3-Switches sogar (idealerweise) in ‚wire speed‘



Segmentierung, allgemeine (Sicherheits-) Aspekte



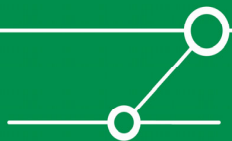
- Üblicherweise lassen sich bei jeder Art der ‚Segmentierung‘ die segmentierten Objekte und gemeinsame Management-Mechanismen unterscheiden (so etwa auch bei VMWare oder UNIX chroot-Umgebungen et.al.)
- Angriffe gegen die gemeinsame Management-Infrastruktur können die Segmentierung ausser Kraft setzen.
- Dieser Aspekt sollte *immer* bedacht werden (auch beim aktuellen Hype zur Server-Virtualisierung/“Konsolidierung“)!



... und ihre Anwendung auf VLANs



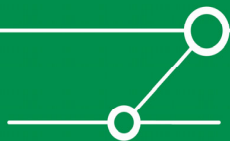
- VLANs wurden *nicht* für Security-Zwecke entwickelt...
- ... werden aber oft genau dafür eingesetzt.
- Segmentierungs-Objekte sind dabei die einzelnen VLANs selbst.
- Die „gemeinsame Management-Infrastruktur“ sind die Switches, ihre Verbindungen untereinander (Cisco: *Trunks*) und zugehörige Protokolle (Cisco: DTP, VTP).



Grundlagen Trunking

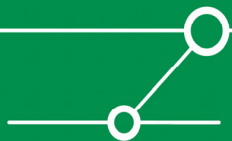
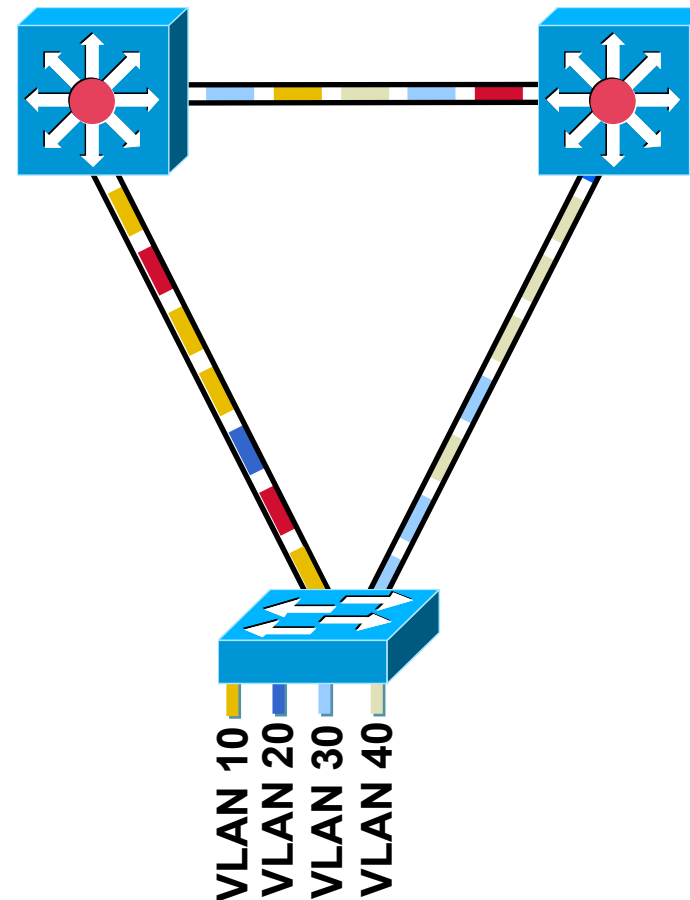


- VLANs sind zunächst nur lokal pro Switch definiert und bekannt.
- Trunk Ports dienen der Übertragung von VLAN-Informationen von Netzwerk-Verkehr zwischen Netzwerk-Devices (von Switches zu anderen Switches/ Routern).
- Ein Port eines Switches ist meist entweder ein *Access Port* oder ein *Trunk Port*.
- Ein Trunk Port ist per default Mitglied aller VLANs eines Switches. Es kann aber beschränkt werden, welche VLANs über den Trunk transportiert werden.
- Trunks werden entweder manuell konfiguriert oder können (bei Cisco) zwischen Switches ausgehandelt werden (per DTP, *Dynamic Trunking Protocol*).



Grundlagen Trunking

- Mithilfe der Trunk Ports können VLANs über mehrere Switches hinweg gebildet werden.



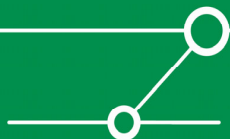
Grundlagen DTP



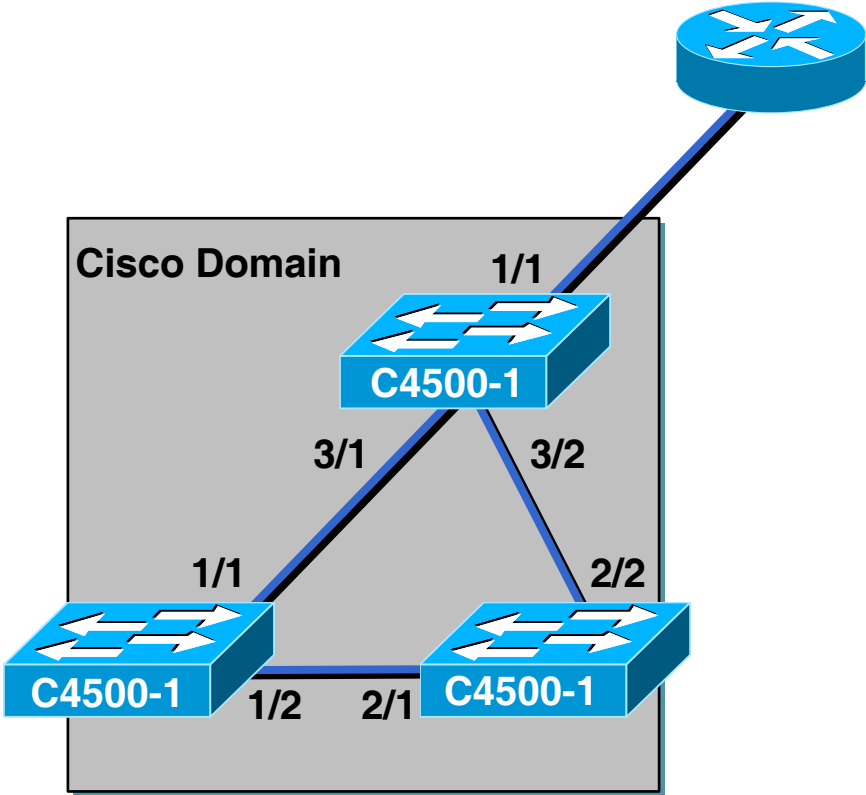
- Viele Cisco Switches (Ausnahme etwa 2900XL/3500XL) unterstützen ein proprietäres Protokoll, das die dynamische Aushandlung von Trunks gestattet:
das *Dynamic Trunking Protocol* (DTP).

Ein Port kann dabei verschiedene Modi haben (jeweils CatOS/IOS):

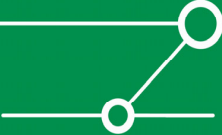
- *On/Mode Trunk*: Port ist definitiv Trunk Port und sendet DTP-Pakete.
 - *Desirable/Mode Dynamic Desirable*: Port sendet DTP-Pakete und wird Trunk, wenn Partner DTP spricht [d.h. im Zustand *On*, *Desirable* oder *Auto* ist).
 - *Auto/Mode Dynamic Auto*: Port sendet DTP-Pakete, wird aber nur Trunk, wenn Partner dediziert will [d.h. im Zustand *On* oder *Desirable* ist].
 - *Nonegotiate/Mode Negotiate*: Aktiviert einen Trunk, deaktiviert aber DTP.
 - *Off/No Switchport Mode Trunk*: Port wird kein Trunk (also Access Port) und spricht auch kein DTP.
-
- Das Nachrichtenformat von DTP ist ähnlich dem von CDP mit HDLC 0x2004.



Grundlagen DTP



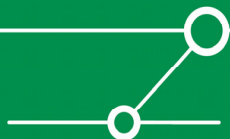
- **Dynamic Trunk Protocol (DTP) sorgt für die Aushandlung von Trunks.**



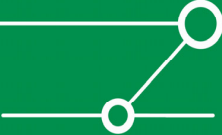
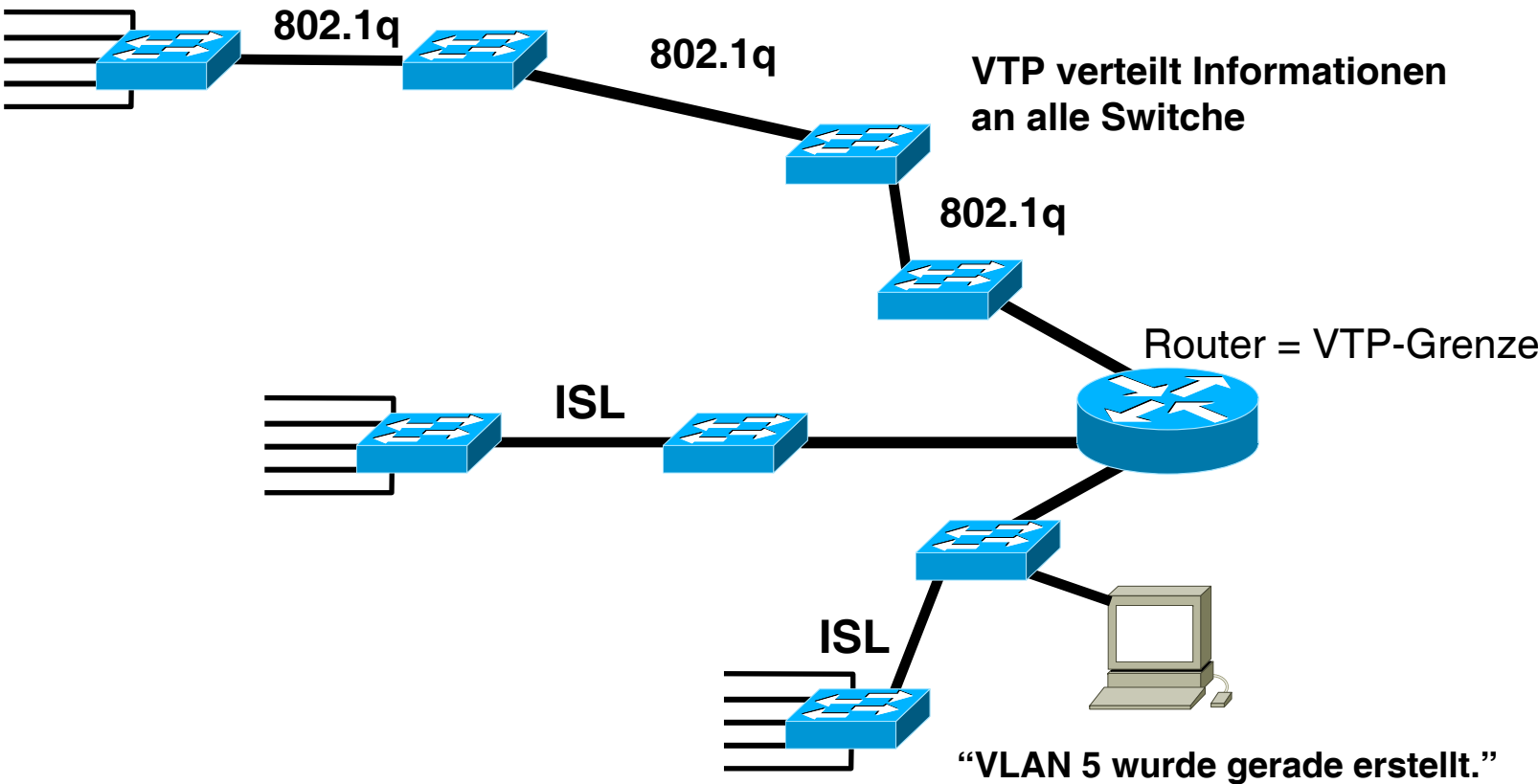
VTP-Grundlagen



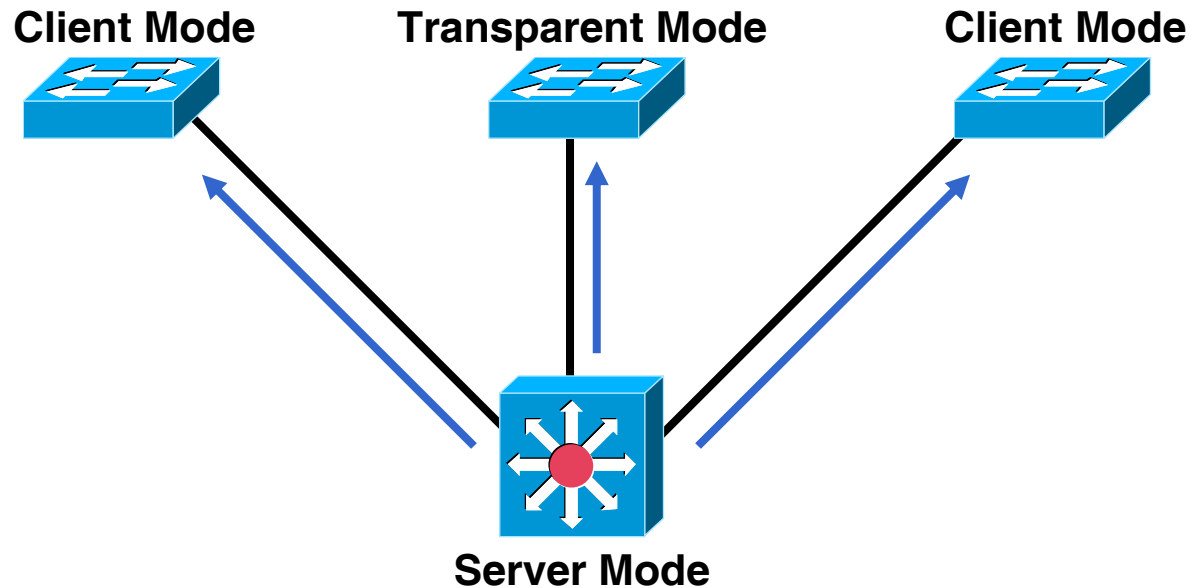
- Während *VLAN Tagging* dazu verwendet wird, einzelne Frames den richtigen VLANs zuzuordnen, dient das *VLAN Trunking Protocol* (VTP) dazu, VLAN-Informationen an sich verschiedenen Switches bekanntzumachen.
- Die Switches versenden dazu über Trunk-Ports VTP-Pakete.
- Nachrichten werden nur zwischen Switches derselben *VTP Domain* ausgetauscht.
- Der Austausch kann durch Passwörter gesichert werden.
- Switches können mit VTP ihre VLAN-Datenbanken synchronisieren und verwenden dazu eine Revisions-Nummer. Achtung: lokale VLANs werden ggf. auf Systemen mit ‚schlechterer‘ Revisions-Nummer gelöscht.
- Switches können in drei verschiedenen *VTP Modi* arbeiten: Server, Client, Transparent.
- VTP kann nicht benötigten Verkehr auf Trunks beschneiden (*VTP Pruning*).
- Das Nachrichtenformat von VTP ist ähnlich dem von CDP, mit SNAP HDLC 0x2003.



VTP-Grundlagen



VTP-Grundlagen



Server Mode
Client Mode
Transparent

= Kann globale VLANs erstellen/löschen
= Kann keine VLANs ändern
= Kann lokale VLANs erstellen/löschen, ignoriert aber *VTP Updates*



Sicherheits-Probleme durch DTP

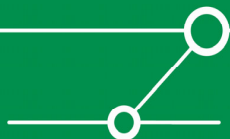


„The key thing to remember about DTP is the default mode on most switches is *Auto.*” [5]

- DTP ist meist per default **aktiviert**.
- Dies ändert sich **nicht** durch die typische Konfig vieler NW-Admins:

```
interface FastEthernet0/2
switchport access vlan 27
spanning-tree portfast
!
interface FastEthernet0/3
switchport access vlan 27
spanning-tree portfast
!
interface FastEthernet0/4
switchport access vlan 27
spanning-tree portfast
```

- => auch auf vermeintlichen Access Ports können Trunk-Verbindungen verhandelt werden.

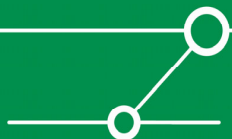


Sicherheits-Probleme durch DTP



Wenn ein Angreifer einen Trunk aushandeln kann...

- kann er sofort den Broadcast- und Multicast-Traffic **aller VLANs** mitlesen (sonstige Default-Konfiguration ohne Einschränkung der *allowed VLANs* und ohne *VTP Pruning* vorausgesetzt).
- kann er ggf. an VTP teilnehmen und dadurch die VLAN-Konfiguration verändern (etwa VLANs erzeugen o. **löschen**).
- kann er per ARP-Spoofing Systeme in **anderen VLANs** attackieren (und damit deren Verkehr mitlesen)!!
[Beispiel: Angreifer kompromittiert Webserver in DMZ und liest von dort Verkehr interner Netze mit.]
- D.h. ein Angriff gegen ein Management-Protokoll (hier DTP) kann die komplette Segmentierung aushebeln.



Demo & Diskussion über Gegenmassnahmen



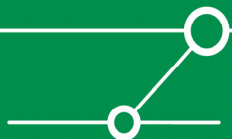
- Ausführlich morgen bei meinem Kollegen Dror-John Röcher ;-))

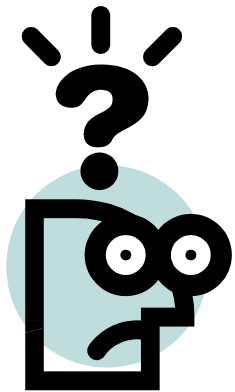


Zusammenfassung



- Netzwerk-Segmentierung kann erheblich zur Sicherheit beitragen.
- Es sollten aber organisatorische und technische Rahmenbedingungen beachtet werden.
- Die typische Segmentierung mit VLANs kann durch Angriffe gegen Management-Protokolle ausgehebelt werden.
- => Geeignete Sicherheits-Massnahmen sind zwingend erforderlich (siehe dazu etwa [3], [4], [6]).





Fragen?

... und Antworten



Danke für Ihre Aufmerksamkeit!



Quellen



- [1] *Quarantine Model Overview for IPv6 Network Security*:
<http://community.roxen.com/developers/idoocs/drafts/draft-kondo-quarantine-overview-01.html>
- [3] Cisco SAFE Blueprint Layer 2 Security:
http://www.cisco.com/en/US/netsol/ns340/ns394/ns171/ns128/networking_solutions_white_paper09186a008014870f.shtml
- [4] NSA Guide Switch Security: http://www.nsa.gov/snac/os/switch-guide-version1_01.pdf
- [5] Cisco Packet Magazine, Artikel „Layer 2 -- The Weakest Link“:
http://www.cisco.com/en/US/about/ac123/ac114/ac173/ac222/about_cisco_packet_feature09186a0080142deb.html
- [6] Catalyst Secure Template: <http://www.cymru.com/gillsr/documents/catalyst-secure-template.htm>

- Allgemeiner Literaturhinweis zu Angriffstechniken (auch gegen Devices):
Dominick Baier/Enno Rey/Michael Thumann: Mehr IT-Sicherheit durch Pen-Tests [Vieweg-Verlag, ISBN 3528058390].

