Workshop System Management

Tobias Lerch, Yanick Eberle, Pascal Schwarz

11. März 2013

1 Netzwerk

1.1 Netzwerkdiagramm

1.2 IP Dual-Stack Konzept

1.2.1 IPv4

Wir unterscheiden zwischen drei verschiedenen Netzwerke. Das interne Netzwerk, das DMZ Netzwerk und das öffentliche Netzwerk. Wir verwenden für die DMZ und das interne Netzwerk verschiedene Netzwerkklassen um die Netze schnell unterscheiden zu können. Folgende IP-Adressierung und Maskierung werden wir verwenden.

Internes Netzwerk
VLAN 10 Server: 10.0.10.0 255.255.255.0 Gateway 10.0.10.1
VLAN 20 Administratoren: 10.0.20.0 255.255.255.0 Gateway 10.0.20.1
VLAN 30 Entwicklung: 10.0.30.0 255.255.255.0 Gatetway 10.0.30.1
VLAN 40 Verkauf: 10.0.40.0 255.255.255.0 Gatetway 10.0.40.1
VPN Clients: 10.0.99.0 255.255.255.0
Infrastructure LAN: 10.100.0.0 255.255.255.252

DMZ
DMZ LAN: 172.16.0.0 255.255.255.0 Gateway 172.16.0.1

Internet
WAN: 209.165.50.0 255.255.255.0 Gateway 209.165.50.1

1.2.2 IPv6

Da die Hosts über das Internet direkt erreichbar sein sollen, werden wir globale IPv6 Adressen mit dem Site Prefix /64 verwenden

Internes Netzwerk
VLAN 10 Server: 2005:2013:FF:A10::/64 Gateway2005:2013:FF:A10::1
VLAN 20 Administratoren: 2005:2013:FF:A20::/64 Gateway 2005:2013:FF:A20::1
VLAN 30 Entwicklung: 2005:2013:FF:A30::/64 Gateway 2005:2013:FF:A30::1
VLAN 40 Verkauf: 2005:2013:FF:A40::/64 Gateway 2005:2013:FF:A40::1
Infrastructure LAN: 2005:2013:FF:A0::/64

DMZ
DMZ LAN: 2005:2013:FF:B0::/64 Gateway 2005:2013:FF:B0::1/64

Internet
WAN: 2005:209:165:50::/64 Gateway 2005:209:165:50::1/64

1.3 Routing

1.3.1 Core Router

Der Core Router hat nur default-routen konfiguriert. Sämtlicher Datenverkehr wird an die Firewall gesendet.
IPv4: 0.0.0.0 0.0.0.0 next Hop 10.100.0.2
IPv6: ::/0 next Hop 2005:2013:FF:A0::2

1.3.2 Firewall

Die default Route auf der Firewall würde normalerweise auf den Router des Service Providers weitergeleitet. Da wir in der Simulation aber keinen solchen haben, werden keine default Routen konfiguriert. Die Firewall sendet somit nur den Verkehr für das interne Netzwerk an den Core Router.
IPv4: 10.0.0.0 255.255.0.0 next Hop 10.100.0.1 (Die einzelnen VLANs wurden hier zu einem /16 Netz zusammengefasst)
IPv6: 2005:2013:FF:A10::/64 next Hop 2005:2013:FF:A0::1
2005:2013:FF:A20::/64 next Hop 2005:2013:FF:A0::1
2005:2013:FF:A30::/64 next Hop 2005:2013:FF:A0::1
2005:2013:FF:A40::/64 next Hop 2005:2013:FF:A0::1

1.4 NAT

Network Address Translation wird für IPv4 verwendet um den internen Clients Zugriff ins Internet zu gewähren und um den Webserver in der DMZ vom Internet aus zugänglich zu machen. Für den Internetzugriff der Clients wird ein Port Address Translation (PAT) konfiguriert, damit nur eine Public IP-Adresse verwendet werden muss. Für den Webserver wird ein statisches NAT mit einer zusätzlichen Public IP-Adresse konfiguriert.

Webserver: statisches NAT interne IP: 172.16.0.11 - öffentliche IP: 209.165.50.2
Interne Hosts: dynamisches NAT overload: interner Range: 10.0.0.0 255.255.0.0 - öffentliche IP 209.165.50.1 (Outside IF IP der Firewall)

1.5 VTP

1.6 Spanning-Tree

1.7 VPN IPsec Remote Access

1.8 Server

Name OS IP Gateway Services
WOSMGR1LANSRV Windows Server 2008 R2 10.0.10.21 10.0.10.1 AD / DNS / DHCP / Fileserver
WOSMGR1LANAdmin Windows 7 10.0.20.21 10.0.20.1

WOSMGR1LANEntwicklung Windows 7 10.0.30.21 10.0.30.1
WOSMGR1LANVerkauf Windows 7 10.0.40.21 10.0.40.1
WOSMGR1DMZSRV Windows Server 2008 R2 172.16.0.21 172.16.0.1 HTTP / HTTPS / FTP
WOSMGR1INETSRV Windows Server 2008 R2 209.165.50.21 209.165.50.1 HTTP / HTTPS / FTP
WOSMGR1INETPC Windows 7 209.165.50.22 209.165.50.1

2 Sicherheit

2.1 Konzept

Bei der Konfiguration des Firewalls sollten Sie sich besonders überlegen und explizit begründen:
a) Welche Dienste allen authentifizierten VLAN-Benutzern zur Verfügung stehen sollten;
b) Welche Teile der Firewall-Konfiguration dem Switch 3560 delegiert werden dürfen;
c) Nach welchem Prinzip (stateless/stateful) der Firewall konzipiert werden soll;
d) Welche Bedrohung mit welcher Firewall-Konfiguration abgewehrt werden soll.

— Low, Mediam und High Security

2.2 Firewall

ACL's

3 Bedrohungsmodel

3.1 TCP DoS (Syn-Flooding)

3.1.1 Bedrohung

Ein Angreifer sendet eine Broadcast Anfrage

3.1.2 Gegenmassnahme

3.2 ICMP 'smurf attack': Denial of Service

3.2.1 Bedrohung

Ein Angreifer sendet ein ICMP Packet mit einer Echo-Anfrage an eine oder mehrere Broadcasts und verwendet als Absenderadresse die IP Adresse des Servers (Opfer). Die Broadcastanfrage wird an alle Hosts in betroffenen Netz weitergeleitet. Die Hosts senden daraufhin ein

die Echo-Antwort an den Server (Opfer). Der Server empfängt nun tausende Echo Antworten und stürtzt ab.

3.2.2 Gegenmassnahme

Um diese Attacke abzuwehren kann ICMP blockiert werden.

3.3 Viren / Würmer / Trojaner

3.3.1 Bedrohung

Programme, welche vertrauliche Infomrationen stehlen, Schaden auf den Hosts anrichten oder die Kontrolle über einen Host übernehmen und ihn für eigene Zwecke einsetzen.

3.3.2 Gegenmassnahme

Um sich gegen Viren, Würmer und Trojaner zu schützen, müss ein Anti-Virenprogramm auf jedem Host installiert werden.

3.4 DNS Cache poisoning

3.4.1 Bedrohung

3.4.2 Gegenmassnahme

3.5 Phishing

3.5.1 Bedrohung

3.5.2 Gegenmassnahme

3.6 MAC flooding

3.6.1 Bedrohung

3.6.2 Gegenmassnahme

3.7 ARP spoofing

3.7.1 Bedrohung

3.7.2 Gegenmassnahme

3.8 DHCP

3.8.1 Bedrohung

zusätzlicher DHCP Server eines Users im LAN

3.8.2 Gegenmassnahme