Workshop System Management

Tobias Lerch, Yanick Eberle, Pascal Schwarz

6. 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

2 Sicherheit

2.1 Firewall

2.2 Bedrohungsmodel