

Workshop System Management

Tobias Lerch, Yanick Eberle, Pascal Schwarz

17. März 2013

1 Netzwerk

1.1 Netzwerkdiagramm

1.2 IP Dual-Stack Konzept

1.2.1 IPv4

Wir unterscheiden zwischen drei verschiedenen Netzwerken. 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

!!!!Create Latex Table!!!!

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 Gateway 10.0.30.1

VLAN 40 Verkauf: 10.0.40.0 255.255.255.0 Gateway 10.0.40.1

VPN Clients Admins: 10.0.99.0 255.255.255.128

VPN Clients Users: 10.0.99.128 255.255.255.128

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

!!!!Create Latex Table!!!!

VLAN 10 Server: 2005:2013:FF:A10::/64 Gateway 2005:2013: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

!!!!Create Latex Table!!!!

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

Internet

!!!!Create Latex Table!!!!

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.

!!!!Create Latex Table!!!!

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.

!!!!Create Latex Table!!!!

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: 172.16.0.21 - 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)

Ausgenommen vom NAT ist die Verbindung vom Server Netzwerk (10.0.10.0/24) ins VPN Client Netzwerk (10.0.99.0/24) da sonst keine Verbindung von Remote Client zu Server erstellt werden kann.

1.5 VTP

Das VLAN Trunking Protokoll kommt in unserer Simulation nicht zu Einsatz, da GNS3 keine konfigurierbare Switches anbietet. Im Labor werden wir jedoch mit konfigurierbaren Switches arbeiten und VTP einsetzen. Der Core Router wird dabei der VTP Server sein und alle VLAN Informationen an die Switches verteilen.

1.6 Spanning-Tree

Spanning-Tree musste in der Simulation nicht berücksichtigt werden. Das Netzwerk ist sehr einfach aufgebaut und die Verbindung zwischen Core Router und Firewall benötigt keinen Spanning-Tree.

1.7 VPN IPsec Remote Access

Der Zugriff auf das interne Netzwerk für externe Mitarbeiter erfolgt über den IPsec VPN Client. Beim Zugriff unterscheiden wir zwischen Administratoren und Mitarbeiter. Der Zugriff als Mitarbeiter kann somit stärker eingeschränkt werden als ein Administrator. In der Simulation haben wir keine unterschiedlichen Zugriffsmöglichkeiten, die Firewall wurde aber für diesen Fall konfiguriert. Der Remote Access Zugang erfolgt über die IP 209.165.50.1 (Outside IF Firewall) und unterstützt nur IPv4.

IKE Phase 1:

- Authentifizierung: Pre-shared
- Verschlüsselung AES 256-bit
- Hash SHA
- Schlüsselgenerierung Diffie-Hellman Group 2
- Gültigkeit Schlüsse 12h

IKE Phase 2 (Group-Policy):

- Interne Gruppen (VPN_ADMINISTRATOR & VPN_USERS_GROUP)
- DNS-Server 10.0.10.21
- ACL 99: permit ip any 10.0.10.0 255.255.255.0
- Split-Tunneling: 10.0.10.0/24
- Tunnel Protokol IKEv1 & IKEv2
- Default Domain: wosm.com
- IP-Adressen Pools: VPN-ADMIN 10.0.99.0/25, VPN-USERS 10.0.99.128/25

1.8 Serverkonzept

!!!!Create Latex Table!!!!

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

Um die Sicherheit unseres Netzes zu gewährleisten, haben wir uns entschieden verschiedene Sicherheitsstufen zu definieren. Dabei verfolgen wir eine High Security Strategie. Die höchste Sicherheitsstufe 'Stufe 1' gilt für die normalen User. Die zweite Sicherheitsstufe 'Stufe 2' gilt für die Server. Die dritte Sicherheitsstufe 'Stufe 3' gilt für die Administratoren.

Bei der Sicherheitsstufe Stufe 1 wird nur das Nötigste zugelassen und alles andere blockiert. Die User dürfen über Ports 80 und 443 im Internet surfen, sowie FTP Verbindungen über Port 21 und 22 öffnen. Zudem werden eingehende DHCP Antworten über den Port UDP 68 zugelassen.

Bei der Sicherheitsstufe Stufe 2 wird alles zugelassen, was die Server benötigen. Dabei wird aus den VLANs 20, 30 und 40 alles zugelassen. Aus der DMZ wird nur der Port 389 für LDAP zugelassen.

Bei der Sicherheitsstufe Stufe 3 wird zusätzlich zu den in Stufe 1 zugelassenen Ports noch der Port 22 im internen Netz und in die DMZ zur Verwaltung der Netzwerkgeräte zugelassen. Zudem ist ins Internet für die Administratoren alles offen.

Die definierten Sicherheitsstufen wurden mithilfe verschiedener ACL's umgesetzt. Die definierten Regeln (Auflistung oben nicht abschliessend) der ACL's sind im folgenden Kapitel ersichtlich.

Die ACL's werden möglichst nahe an der Quelle angewendet. Somit sind alle ACL's welche den Zugriff der verschiedenen internen VLAN's in irgend ein anderes Netz regeln auf dem Core Switch auf den Interfaces in Richtung 'in' angewendet. Alle ACL's die den Zugriff in die DMZ, resp. von der DMZ in ein anderes Netz regeln auf der ASA angewendet. Alle ACL's die den eingehenden Traffic aus dem Internet regeln sind ebenfalls auf der ASA angewendet.

Mit einer Stateful Firewall ist ein höherer Konfigurationsaufwand verbunden, aber gleichzeitig auch eine höhere Sicherheit. Da wir eine High Security Strategie verfolgen, ist die Stateful Variante besser geeignet für unsere Zwecke.

2.2 Firewall

Auf der Firewall wurden 3 Access Lists definiert. DMZ_in, Inside_in und Outside_in. Aus dem DMZ-Netzwerk sind folgende Verbindungen erlaubt.

- host 172.16.0.21 zu host 10.0.10.21, Port tcp 389 (ldap)
- host 172.16.0.21 ins Internet, Ports tcp 80, 443, 21, 22 & udp 53

Aus dem Internet sind folgende Verbindungen erlaubt.

- any zu host 172.16.0.21, Ports tcp 80, 433, 21, 22, 48999 - 49999

Da die Access Lists nahe an der Quelle implementiert wurden, gibt es in der inside_in ACL keine Einschränkungen (permit ip any any). Alle anderen Verbindungen werden nicht zugelassen.

3 Bedrohungsmodel

3.1 TCP DoS (SYN-Flooding)

3.1.1 Bedrohung

Beim TCP 3-Way Handshake wird zuerst eine Anfrage an einen Server gesendet, indem ein TCP Paket mit dem Flag SYN verschickt wird. Der Server als Empfänger dieses TCP SYN Pakets verarbeitet dieses und sendet ein TCP Paket mit den Flags SYN und ACK zurück. Er merkt sich dabei in einer SYN-Liste, mit wem er ein 3-Way Handshake begonnen hat. Wenn der Initiator der Verbindung das TCP Paket mit den Flags SYN und ACK empfängt, verarbeitet er dieses und sendet zur Bestätigung ein Paket mit dem Flag ACK. Sobald der Server das Paket mit dem Flag ACK erhalten hat, wird der Eintrag in der SYN-Liste gelöscht. Ein Angreifer sendet 100 SYN-Anfragen pro Sekunde an einen bestimmten Server. Dabei setzt er eine andere Source IP Adresse, sodass die Antwort nicht zum Angreifer kommt. Da sich der Server merkt, mit wem er einen 3-Way Handshake begonnen, diese aber nicht abschliessen kann, da nie eine Bestätigung mit dem Flag ACK eintrifft, wird der Arbeitsspeicher des Server gefüllt. Sobald der Speicher gefüllt ist, kann dieser keine weiteren Verbindungen mehr aufnehmen oder stürzt ab.

3.1.2 Gegenmassnahme

Um einen Webserver vor diesem Angriff zu schützen, kann die Anzahl der Verbindungen in der Warteschlange vergrößert werden. Zudem kann das Timeout reduziert werden um Speicher freizugeben. Weiter kann auf der ASA SYN Cookies oder SYN Cache aktiviert und limitiert werden. Dadurch sind die Server hinter der ASA vor SYN-Flooding Attacks geschützt.

3.2 ICMP 'smurf attack': Denial of Service

3.2.1 Bedrohung

Ein Angreifer sendet ein ICMP Paket mit einer Echo-Anfrage an eine oder mehrere Broadcasts und verwendet als Absenderadresse die IP Adresse des Servers (Opfer). Die Broadcast-anfrage wird an alle Hosts in betroffenen Netz weitergeleitet. Die Hosts senden daraufhin ein Echo-Antwort an den Server (Opfer). Der Server empfängt nun so viele Echo Antworten dass der Server nicht mehr reagiert und abstürzt.

3.2.2 Gegenmassnahme

Um diese Attacke abzuwehren, kann ICMP blockiert werden. So ist sichergestellt, dass keine Echo Antworten den Server erreichen.

3.3 Viren / Würmer / Trojaner

3.3.1 Bedrohung

Programme, welche vertrauliche Informationen stehlen, Schaden auf den Hosts anrichten oder die Kontrolle über einen Host übernehmen und ihn für eigene Zwecke einsetzen. Zudem können diese Programme zum Beispiel als SMTP Relay fungieren und SPAM Nachrichten versenden, wodurch die Public IP auf einer Blackliste gelistet werden kann.

3.3.2 Gegenmassnahme

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

3.4 DNS Cache poisoning

3.4.1 Bedrohung

Ein Angreifer bringt bei einem DNS Server gefälschte Daten in den Cache. Wenn nun ein Benutzer auf diese Daten zugreift, wird dieser auf manipulierte Seiten weitergeleitet. Der Angreifer kann nun mit Phishing Daten des Benutzer stehlen.

3.4.2 Gegenmassnahme

Der beste Schutz gegen diesen Angriff ist der Einsatz von DNSSEC, welcher mit Authentifizierung und Integrität arbeitet.

3.5 Phishing

3.5.1 Bedrohung

Beim Phishing versucht ein Angreifer durch gefälschte Websites, SPAM Mails oder andere Methoden an Daten eines Internet-Benutzer zu gelangen. So kann ein Angreifer an Kreditkarteninformationen oder weitere Daten kommen und einen erheblichen finanziellen Schaden anrichten.

3.5.2 Gegenmassnahme

Leider gibt es gegen diese Attacke keine effektive Schutzmassnahme. Um sich möglichst gut gegen diese Attacke zu schützen, müssen die Benutzer geschult werden. Zudem kann ein SPAM Filter Mails von potentiellen Angreifern löschen oder markieren, sodass sich der Benutzer dem Risiko bewusst ist.

3.6 MAC flooding

3.6.1 Bedrohung

Ein Angreifer sendet viele ARP Antworten. Dabei setzt er immer eine andere MAC Adresse. Wenn die Index Tabelle des Switches voll ist, schaltet dieser in den Hub Modus um und sendet alle Pakete jedem angeschlossenen Gerät. Nun kann der Angreifer jegliche Kommunikation über diesen Switch mithören.

3.6.2 Gegenmassnahme

Um sich gegen diese Attacke zu schützen, kann auf dem Switch definiert werden, dass er ausschalten soll, wenn die Index Tabelle voll ist. Dadurch ist zwar ein Unterbruch im Netz vorhanden, aber der Angreifer kann nicht mithören.

Eine noch besserer Schutz ist, wenn die Port Security auf dem Switch aktiviert und konfiguriert wird. Dadurch hat kein Angreifer die Möglichkeit die Index Tabelle des Switches zu füllen.

3.7 ARP spoofing

3.7.1 Bedrohung

Ein Angreifer sendet ARP Antworten mit den IP Adressen der Opfer und seiner eigenen MAC Adresse. Der Switch merkt sich nun dass die IP Adressen zur MAC Adresse des Angreifers gehören. Wenn nun ein Opfer ein Paket sendet, wird dieses vom Switch zum Angreifer weitergeleitet. Der Angreifer hat nun Einblick in die Daten, kann diese allenfalls verändern und leitet dieses schliesslich weiter zum effektiven Ziel, sodass niemand etwas davon mitbekommt.

3.7.2 Gegenmassnahme

Um sich gegen diese Attacke zu schützen, kann die Port Security auf dem Switch aktiviert werden, dadurch hat ein potentieller Angreifer gar keine Möglichkeit sich ins interne Netz einzubinden.

3.8 DHCP

3.8.1 Bedrohung

Eine Person mit Zugriff auf ein Netzkabel im internen Netz verbindet einen zusätzlichen, nicht autorisierten DHCP Server. Wenn der zusätzliche DHCP Server schnellere Antwortzeiten hat als der offizielle DHCP Server, erhalten die Clients nun eine IP des nicht autorisierten DHCP Server, wodurch diese nicht mehr auf die interne Infrastruktur zugreifen können.

3.8.2 Gegenmassnahme

Um dies zu verhindern, kann der Port 68 für DHCP Antworten blockiert werden (ausser vom offiziellen DHCP Server). Dadurch ist sichergestellt, dass kein zusätzlicher DHCP Server IP Adressen im internen Netz verteilen kann.

3.9 Überblick

Hier noch einmal ein Überblick der beschriebenen Bedrohungen inkl. Priorisierung und Markierung, gegen welche wir uns schützen:

!!!!Create Latex Table!!!!

Ranking Eintrittswahrscheinlichkeit Schweregrad Bedrohung Schutz umgesetzt

1 hoch hoch ICMP 'smurf attack': Denial of Service ja

2 hoch mittel Viren / Würmer / Trojaner nein

3 mittel hoch TCP DoS (SYN-Flooding) ja

4 mittel hoch DNS Cache poisoning nein

5 hoch niedrig Phishing nein

6 niedrig hoch DHCP ja

7 niedrig mittel MAC flooding nein

8 niedrig mittel ARP spoofing nein

3.10 ACL gegen Attacken

3.10.1 ICMP 'smurf attack': Denial of Service

3.10.2 TCP DoS (SYN-Flooding)

3.10.3 DHCP