

Workshop System Management

Tobias Lerch, Yanick Eberle, Pascal Schwarz

18. März 2013

Inhaltsverzeichnis

1. Netzwerk	4
1.1. Netzwerkdiagramm	4
1.2. IP Dual-Stack Konzept	4
1.2.1. IPv4	4
1.2.2. IPv6	5
1.3. Adressvergabe an Clients	5
1.3.1. IPv4	5
1.3.2. IPv6	5
1.4. Routing	6
1.4.1. Core Router	6
1.4.2. Firewall	7
1.5. NAT	7
1.6. VTP	7
1.7. Spanning-Tree	7
1.8. VPN IPsec Remote Access	8
1.9. Serverkonzept	8
2. Sicherheit	9
2.1. Konzept	9
2.2. Firewall	9
2.2.1. ACL auf Core-Router	9
2.2.2. ACL auf ASA	10
3. Bedrohungsmodell	10
3.1. TCP DoS (SYN-Flooding)	10
3.1.1. Bedrohung	10
3.1.2. Gegenmassnahme	11
3.2. ICMP 'smurf attack': Denial of Service	11
3.2.1. Bedrohung	11
3.2.2. Gegenmassnahme	11
3.3. Viren / Würmer / Trojaner	11
3.3.1. Bedrohung	11
3.3.2. Gegenmassnahme	11
3.4. DNS Cache poisoning	12
3.4.1. Bedrohung	12
3.4.2. Gegenmassnahme	12
3.5. Phishing	12
3.5.1. Bedrohung	12
3.5.2. Gegenmassnahme	12
3.6. MAC flooding	12
3.6.1. Bedrohung	12
3.6.2. Gegenmassnahme	13
3.7. ARP spoofing	13
3.7.1. Bedrohung	13
3.7.2. Gegenmassnahme	13
3.8. Rogue DHCP	13
3.8.1. Bedrohung	13

3.8.2. Gegenmassnahme	13
3.9. Überblick	13
3.10. ACL gegen Attacken	14
3.10.1. ICMP ‘smurf attack’: Denial of Service	14
3.10.2. TCP DoS (SYN-Flooding)	14
3.10.3. DHCP IPv4	14
3.10.4. Autoconfiguration IPv6	14
Anhang	15
A. Konfiguration Core	15
B. Konfiguration ASA	21

1. Netzwerk

1.1. Netzwerkdiagramm

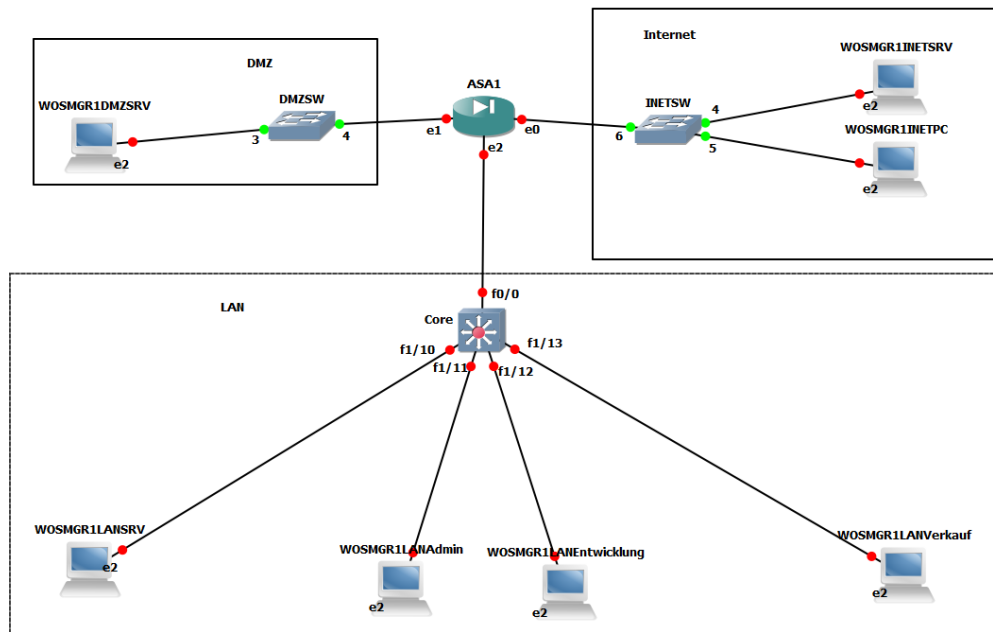


Abbildung 1: Netzwerk

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.

VLAN	Funktion	IPv4 Range	IPv4 Gateway
10	Server	10.0.10.0/24	10.0.10.1
20	Administratoren	10.0.20.0/24	10.0.20.1
30	Entwicklung	10.0.30.0/24	10.0.30.1
40	Verkauf	10.0.40.0/24	10.0.40.1
n/a	VPN Clients	10.0.99.0/24	n/a
n/a	Infrastructure	10.100.0.0/30	n/a
n/a	DMZ	172.16.0.0/24	172.16.0.1
n/a	WAN	209.165.50.0/24	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.

VLAN	Funktion	IPv6 Range	IPv6 Gateway
10	Server	2005:2013:FF:A10::/64	2005:2013:FF:A10::1
20	Administratoren	2005:2013:FF:A20::/64	2005:2013:FF:A20::1
30	Entwicklung	2005:2013:FF:A30::/64	2005:2013:FF:A30::1
40	Verkauf	2005:2013:FF:A40::/64	2005:2013:FF:A40::1
n/a	Infrastructure	2005:2013:FF:A0::/64	n/a
n/a	DMZ	2005:2013:FF:B0::/64	2005:2013:FF:B0::1/64
n/a	WAN	2005:209:165:50::/64	2005:209:165:50::1/64

1.3. Adressvergabe an Clients

1.3.1. IPv4

Die Clients stellen reguläre DHCP-Anfragen. Um die Leases und Bereichsoptionen zentral und (einigermassen) angenehm über eine grafische Schnittstelle verwalten zu können, wird der Core-Router so konfiguriert, dass er die Anfragen an den internen Domänencontroller und DHCP-Server (INTSRV in VLAN10) weiterleitet. Der Router setzt dabei ein Flag in der Anfrage, welches es dem DHCP-Server erlaubt, festzustellen aus welchem Bereich die Anfrage kam. Nur so kann der Server beispielsweise einem Client aus dem Adminnetz eine IP aus dem Admin-Bereich zuweisen.

Der folgende Konfigurationsausschnitt zeigt die notwendigen Optionen (IPv6-betreffende Einstellungen entfernt):

```
1 interface Vlan20
2   description *** VLAN Admin ***
3   ip address 10.0.20.1 255.255.255.0
4   ip access-group ADMIN in
5   ip helper-address 10.0.10.21
```

Der Befehl „ip helper address“ gibt an, wohin die DHCP-Anfrage weitergeleitet werden soll.

1.3.2. IPv6

Für die automatische Konfiguration der Client-Adressen für IPv6 kommen mehrere Möglichkeiten in Betracht:

Autokonfiguration ohne DHCP IPv6 sieht vor, dass Router Clients direkt das zu verwendende Netzwerkprefix angeben können und Clients sich dann mittels EUI-64 eine Adresse generieren. Da EUI-64 die (weltweit eindeutige) MAC-Adresse miteinbezieht, sind Adresskonflikte ausgeschlossen. Die Clients erfahren über Router-Advertisements, welche Netze sie über welche Router erreichen können. Leider ist keine Möglichkeit vorgesehen, den Clients mitzuteilen, welchen DNS-Server sie verwenden sollen. Somit kann dieser Ansatz alleine aktuell das Problem der Adressvergabe nicht abschliessend lösen.

DHCPv6 stateful Diese Variante funktioniert sehr ähnlich wie die klassische DHCP Adressvergabe in IPv4-Netzen. Der Client fragt per Multicast (Broadcast-Adressen wurden in IPv6 abgeschafft) nach DHCP-Servern und „bestellt“ sich eine Adresse. Die Angabe von weiteren Optionen, wie eine Liste der DNS-Server ist genau auf die selbe Art und Weise möglich, wie dies bereits in IPv4-Netzen der Fall war. Eine Einschränkung ist bei unserer Konfiguration allerdings ins Gewicht gefallen: Der DHCP-Server kann den Clients keinen Default-Gateway angeben, eine entsprechende Option ist derzeit im Protokoll nicht vorgesehen.

DHCPv6 stateless Diese Variante vereint die Stärken der beiden zuvor genannten Varianten der Adressvergabe. Die Konfiguration der IPv6-Adresse sowie des Gateways erfolgt per Router-Advertisements zwischen Router und Client. In der Antwort zur Router-Solicitation-Anfrage des Clients gibt der Router dem Client des Weiteren an, dass er weitere Informationen per DHCPv6 erfragen soll. Als Antwort auf die DHCP-Anfrage erhält der Client dann Optionen wie eine DNS-Serverliste oder den Domännennamen. Die Bezeichnung „stateless“ rührt daher, dass der Server keine Informationen (Lease) zu den Clients speichern muss.

Auch dieser Ansatz soll mit einem Auszug der Schnittstellenkonfiguration verdeutlicht werden (IPv4 betreffende Konfigurationen entfernt):

```
1 interface Vlan20
2   description *** VLAN Admin ***
3   ipv6 address 2005:2013:FF:A20::1/64
4   ipv6 traffic-filter ADMINv6 in
5   ipv6 nd other-config-flag
6   ipv6 dhcp relay destination 2005:2013:FF:A10::21
```

Die Option „ipv6 nd other-config-flag“ gibt an, dass der Router Clients darauf hinweisen soll, dass weitere Informationen über DHCPv6 erhalten werden können. Eine andere Einstellung hier wäre „ipv6 nd managed-config-flag“ - dies würde den Client auffordern, auch seine IP-Adresse per DHCPv6 zu erfragen.

„ipv6 dhcp relay destination“ gibt, analog zu der „helper-adress“ bei IPv4, an, wohin DHCP-Anfragen weitergeleitet werden sollen.

Des Weiteren ist zu beachten, dass eintreffende „Router-Solicitation“-Anfragen der Clients nicht durch die ACL geblockt werden. Falls dies dennoch der Fall ist, erhält der Client die IPv6-Route erst nach einiger Zeit, da der Router von sich aus periodisch Router-Advertisement verschickt.

1.4. Routing

1.4.1. Core Router

Der Core Router hat nur default-routen konfiguriert. Sämtlicher Datenverkehr, der nicht in ein lokal angeschlossenes Netz soll, wird an die Firewall gesendet.

Zielnetz	Next Hop
0.0.0.0/0	10.100.0.2
::/0	2005:2013:FF:A0::2

1.4.2. Firewall

Die default Route auf der Firewall würde normalerweise auf den Router des Service Providers zeigen. 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.

Zielnetz	Next Hop
10.0.0.0/16 (Supernet)	10.100.0.1
2005:2013:FF:A10::/64	2005:2013:FF:A0::1
2005:2013:FF:A20::/64	2005:2013:FF:A0::1
2005:2013:FF:A30::/64	2005:2013:FF:A0::1
2005:2013:FF:A40::/64	2005:2013:FF:A0::1

1.5. 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 eine 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: 10.0.0.0/16 - 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.

1.6. 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.

1.7. 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.

1.8. 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

1.9. Serverkonzept

Name	OS	IPv4	IPv6	Services
LANSRV	Windows Server 2008 R2	10.0.10.21	2005:2013:ff:a10::21	AD, DNS, DHCP, Fileserver
LANAdmin	Windows 7	10.0.20.21	2005:2013:ff:a20::21	Client Admin
LANEntwicklung	Windows 7	10.0.30.21	2005:2013:ff:a30::21	Client Entwicklung
LANVerkauf	Windows 7	10.0.40.21	2005:2013:ff:a40::21	Client Verkauf
DMZSRV	Windows Server 2008 R2	172.16.0.21	2005:2013:ff:b0::21	HTTP, HTTPS, FTP
INETSrv	Windows Server 2008 R2	209.165.50.21	2005:209:165:50::21	HTTP, HTTPS, FTP
INETPC	Windows 7	209.165.50.22	2005:209:165:50::22	Client Extern

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 20 öffnen. Zudem werden eingehende DHCP Anfragen 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 beim Internetzugang für die Administratoren alles offen.

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

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

Mit einer Stateful Firewall sinkt einerseits der Konfigurationsaufwand und gleichzeitig kann eine höhere Sicherheit erreicht werden. Da wir eine High Security Strategie verfolgen, ist die Stateful Variante besser geeignet für unsere Zwecke.

2.2. Firewall

2.2.1. ACL auf Core-Router

Auf diesem Router sind ACL für alle angeschlossenen VLANs definiert. Die folgende Tabelle liefert einen Überblick, die kompletten ACL sind im Anhang dieser Dokumentation zu finden.

Name	Interface/Richtung	Anmerkung
INTSRV	VLAN 10 / in	Reglementiert IPv4 Traffic, der aus dem Servernetz verschickt werden darf.
INTSRVv6	VLAN 10 / in	Reglementiert IPv6 Traffic, der aus dem Servernetz verschickt werden darf.

Fortführung auf nächster Seite...

Name	Interface/Richtung	Anmerkung
ADMIN	VLAN 20 / in	Reglementiert IPv4 Traffic, der aus dem Adminnetz verschickt werden darf.
ADMINv6	VLAN 20 / in	Reglementiert IPv6 Traffic, der aus dem Adminnetz verschickt werden darf.
DEV	VLAN 30 / in	Reglementiert IPv4 Traffic, der aus dem Entwicklungsnetz verschickt werden darf.
DEVv6	VLAN 30 / in	Reglementiert IPv6 Traffic, der aus dem Entwicklungsnetz verschickt werden darf.
VERKAUF	VLAN 40 / in	Reglementiert IPv4 Traffic, der aus dem Verkaufsnetz verschickt werden darf.
VERKAUFv6	VLAN 40 / in	Reglementiert IPv6 Traffic, der aus dem Verkaufsnetz verschickt werden darf.

2.2.2. ACL auf ASA

Auf der Firewall wurden jeweils 3 Access Lists definiert. Diese werden auf den jeweiligen Interfaces angewendet. Die kompletten Access-lists sind im Anhang zu finden.

Name	Interface/Richtung	Anmerkung
dmz_in	dmz / in	IPv4 Traffic, der aus dem DMZ-Netzwerk verschickt werden darf.
dmz_in_v6	dmz / in	IPv6 Traffic, der aus dem DMZ-Netzwerk verschickt werden darf.
inside_in	inside / in	IPv4 Traffic, der aus dem internen Netzwerk verschickt werden darf.
inside_in_v6	inside / in	IPv6 Traffic, der aus dem internen Netzwerk verschickt werden darf.
outside_in	outside / in	IPv4 Traffic, der aus dem Internet verschickt werden darf.
outside_in_v6	outside / in	IPv6 Traffic, der aus dem Internet verschickt werden darf.

3. Bedrohungsmodell

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 Falgs 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 Packet 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 auf der ASA eine Policy erstellt werden, welche die maximale Anzahl Verbindungen und halb offener Verbindungen limitiert. Zudem können Timeouts gesetzt werden, wie lange eine Verbindung in welchem Status sein darf (halb offen, offen, halb geschlossen). Auf einem normalen Router kann mit SYN-Cookies oder SYN-Cache gearbeitet 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 Packet 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 den Datenverkehr 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 Anfreifer gar keine Möglichkeit sich ins interne Netz einzubinden.

3.8. Rogue 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 interne Netz verteilen kann.

3.9. Überblick

Rang	Wahrscheinlichkeit	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	Rogue 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 IPv4

Die ACL für die internen Client-VLANs verhindert das Versenden einer Antwort auf eine DHCP-Anfrage. Um die Beantwortung aus dem Servernetz zu erlauben wurden die folgenden Regeln angewendet:

```

1 permit udp 10.0.10.0 0.0.0.255 eq 67 10.0.20.1 0.0.0.0 eq 67
2 permit udp 10.0.10.0 0.0.0.255 eq 67 10.0.30.1 0.0.0.0 eq 67
3 permit udp 10.0.10.0 0.0.0.255 eq 67 10.0.40.1 0.0.0.0 eq 67

```

Bei der Situation, einen DHCP-Server innerhalb eines Client VLANs daran zu hindern, anderen Clients im selben VLAN eine Adresse zuzuteilen, müsste eine ACL auch auf den Switches angewendet werden (Richtung: in), welche den Datenverkehr über UDP von Quellport 67 an Zielport 68 nicht erlaubt.

3.10.4. Autoconfiguration IPv6

Bei IPv6 ist dieses Problem etwas anders zu handhaben. Es muss verhindert werden, dass Clients Router-Advertisements verschicken können. Dies kann durch einen ACL-Eintrag der folgenden Art umgesetzt werden (die ACL müsste in Richtung *in* auf dem zu den Clients führenden IFs angewendet werden):

```

1 deny icmp any any router-advertisement

```

Analog IPv4 muss ebenfalls der Traffic von UDP Quellport 547 an den Zielport 546 aus den Client-Netzen unterbunden werden.

A. Konfiguration Core

```
1  !
2  !
3  version 12.4
4  service timestamps debug datetime msec
5  service timestamps log datetime msec
6  no service password-encryption
7  !
8  hostname Core
9  !
10 boot-start-marker
11 boot-end-marker
12 !
13 !
14 no aaa new-model
15 memory-size iomem 5
16 ip cef
17 !
18 !
19 !
20 !
21 no ip domain lookup
22 ip domain name lab.local
23 ip auth-proxy max-nodata-conns 3
24 ip admission max-nodata-conns 3
25 !
26 ipv6 unicast-routing
27 !
28 !
29 !
30 !
31 !
32 !
33 !
34 !
35 !
36 !
37 !
38 !
39 !
40 !
41 !
42 !
43 !
44 !
45 !
46 !
47 !
48 interface FastEthernet0/0
49   description *** to R1 ***
50   ip address 10.100.0.1 255.255.255.252
51   speed 100
52   full-duplex
53   ipv6 address 2005:2013:FF:A0::1/64
54 !
55 interface FastEthernet0/1
56   no ip address
57   shutdown
58   duplex auto
59   speed auto
60 !
61 interface FastEthernet1/0
62   switchport access vlan 10
63 !
64 interface FastEthernet1/1
65   switchport access vlan 20
66 !
```

```

67 interface FastEthernet1/2
68   switchport access vlan 30
69   !
70 interface FastEthernet1/3
71   switchport access vlan 40
72   !
73 interface FastEthernet1/4
74   !
75 interface FastEthernet1/5
76   !
77 interface FastEthernet1/6
78   !
79 interface FastEthernet1/7
80   !
81 interface FastEthernet1/8
82   !
83 interface FastEthernet1/9
84   !
85 interface FastEthernet1/10
86   switchport access vlan 10
87   !
88 interface FastEthernet1/11
89   switchport access vlan 20
90   !
91 interface FastEthernet1/12
92   switchport access vlan 30
93   !
94 interface FastEthernet1/13
95   switchport access vlan 40
96   !
97 interface FastEthernet1/14
98   !
99 interface FastEthernet1/15
100  !
101 interface Vlan1
102   no ip address
103   !
104 interface Vlan10
105   description *** VLAN Server ***
106   ip address 10.0.10.1 255.255.255.0
107   ip access-group INTSRV in
108   ip helper-address 10.0.10.21
109   ipv6 address 2005:2013:FF:A10::1/64
110   ipv6 traffic-filter INTSRVv6 in
111   !
112 interface Vlan20
113   description *** VLAN Admin ***
114   ip address 10.0.20.1 255.255.255.0
115   ip access-group ADMIN in
116   ip helper-address 10.0.10.21
117   ipv6 address 2005:2013:FF:A20::1/64
118   ipv6 traffic-filter ADMINv6 in
119   ipv6 nd other-config-flag
120   ipv6 dhcp relay destination 2005:2013:FF:A10::21
121   !
122 interface Vlan30
123   description *** VLAN Entwicklung ***
124   ip address 10.0.30.1 255.255.255.0
125   ip access-group DEV in
126   ip helper-address 10.0.10.21
127   ipv6 address 2005:2013:FF:A30::1/64
128   ipv6 traffic-filter DEVv6 in
129   ipv6 nd other-config-flag
130   ipv6 dhcp relay destination 2005:2013:FF:A10::21
131   !
132 interface Vlan40
133   description *** VLAN Verkauf ***
134   ip address 10.0.40.1 255.255.255.0
135   ip access-group VERKAUF in

```



```

136 ip helper-address 10.0.10.21
137 ipv6 address 2005:2013:FF:A40::1/64
138 ipv6 traffic-filter VERKAUFv6 in
139 ipv6 nd other-config-flag
140 ipv6 dhcp relay destination 2005:2013:FF:A10::21
141 !
142 ip forward-protocol nd
143 ip route 0.0.0.0 0.0.0.0 10.100.0.2
144 !
145 !
146 no ip http server
147 no ip http secure-server
148 !
149 ip access-list extended ADMIN
150 remark admin-dhcp
151 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
152 remark admin-dns
153 permit udp 10.0.20.0 0.0.0.255 host 10.0.10.21 eq domain
154 remark admin-intsrv
155 permit ip 10.0.20.0 0.0.0.255 10.0.10.0 0.0.0.255
156 remark admin-int
157 permit ip 10.0.20.0 0.0.0.255 10.0.30.0 0.0.0.255
158 permit ip 10.0.20.0 0.0.0.255 10.0.40.0 0.0.0.255
159 permit ip 10.0.20.0 0.0.0.255 10.0.99.0 0.0.0.255
160 remark admin-dmzsrv
161 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq www
162 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq 443
163 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq ftp-data
164 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq ftp
165 remark admin-dmzsrv-ftppasv
166 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 gt 48999
167 deny tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 gt 49999
168 remark admin-dmzsw
169 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.2 eq 22
170 remark admin-dmz-end
171 deny ip 10.0.20.0 0.0.0.255 172.16.0.0 0.0.0.255
172 remark admin-network
173 permit ip 10.0.20.0 0.0.0.255 10.0.100.0 0.0.0.255
174 remark admin-inet
175 permit tcp 10.0.20.0 0.0.0.255 any
176 ip access-list extended DEV
177 remark dev-dhcp
178 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
179 remark dev-dns
180 permit udp 10.0.30.0 0.0.0.255 host 10.0.10.21 eq domain
181 remark dev-intsrv
182 permit ip 10.0.30.0 0.0.0.255 host 10.0.10.21
183 remark dev-intsrv-end
184 deny ip 10.0.30.0 0.0.0.255 10.0.10.0 0.0.0.255
185 remark dev-respondadmin
186 permit tcp 10.0.30.0 0.0.0.255 10.0.20.0 0.0.0.255 established
187 remark dev-dmzsrv
188 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq www
189 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq 443
190 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq ftp-data
191 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq ftp
192 remark dev-dmzsrv-ftppasv
193 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 gt 48999
194 deny tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 gt 49999
195 remark dev-dmzsrv-end
196 deny ip 10.0.30.0 0.0.0.255 172.16.0.0 0.0.0.255
197 remark dev-inet
198 permit tcp 10.0.30.0 0.0.0.255 any eq www
199 permit tcp 10.0.30.0 0.0.0.255 any eq 443
200 permit tcp 10.0.30.0 0.0.0.255 any eq ftp-data
201 permit tcp 10.0.30.0 0.0.0.255 any eq ftp
202 ip access-list extended INTSRV
203 remark intsrv-adm
204 permit tcp 10.0.10.0 0.0.0.255 10.0.20.0 0.0.0.255 established

```

```

205 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.20.0 0.0.0.255
206 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.20.1 eq bootps
207 remark intsrv-dev
208 permit tcp 10.0.10.0 0.0.0.255 10.0.30.0 0.0.0.255 established
209 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.30.0 0.0.0.255
210 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.30.1 eq bootps
211 remark intsrv-verkauf
212 permit tcp 10.0.10.0 0.0.0.255 10.0.40.0 0.0.0.255 established
213 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.40.0 0.0.0.255
214 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.40.1 eq bootps
215 remark intsrv-vpn
216 permit tcp 10.0.10.0 0.0.0.255 10.0.99.0 0.0.0.255 established
217 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.99.0 0.0.0.255
218 remark intsrv-lan-end
219 deny ip 10.0.10.0 0.0.0.255 10.0.0.0 0.0.255.255
220 remark intsrv-dmzsrv
221 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq www
222 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq 443
223 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq ftp-data
224 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq ftp
225 remark admin-dmzsrv-ftppasv
226 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 gt 48999
227 deny tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 gt 49999
228 remark intsrv-dmzsrv-respond-radius
229 permit tcp host 10.0.10.21 eq 389 host 172.16.0.21 established
230 remark intsrv-dmzsrv-end
231 deny ip 10.0.10.0 0.0.0.255 172.16.0.0 0.0.0.255
232 remark intsrv-inet
233 permit tcp 10.0.10.0 0.0.0.255 any eq www
234 permit tcp 10.0.10.0 0.0.0.255 any eq 443
235 permit tcp 10.0.10.0 0.0.0.255 any eq ftp-data
236 permit tcp 10.0.10.0 0.0.0.255 any eq ftp
237 permit udp 10.0.10.0 0.0.0.255 any eq domain
238 ip access-list extended VERKAUF
239 remark verkauf-dhcp
240 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
241 remark verkauf-dns
242 permit udp 10.0.40.0 0.0.0.255 host 10.0.10.21 eq domain
243 remark verkauf-intsrv
244 permit ip 10.0.40.0 0.0.0.255 host 10.0.10.21
245 remark verkauf-intsrv-end
246 deny ip 10.0.40.0 0.0.0.255 10.0.10.0 0.0.0.255
247 remark verkauf-respondadmin
248 permit tcp 10.0.40.0 0.0.0.255 10.0.20.0 0.0.0.255 established
249 remark verkauf-dmzsrv
250 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq www
251 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq 443
252 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq ftp-data
253 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq ftp
254 remark verkauf-dmzsrv-ftppasv
255 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 gt 48999
256 deny tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 gt 49999
257 remark verkauf-dmzsrv-end
258 deny ip 10.0.40.0 0.0.0.255 172.16.0.0 0.0.0.255
259 remark verkauf-inet
260 permit tcp 10.0.40.0 0.0.0.255 any eq www
261 permit tcp 10.0.40.0 0.0.0.255 any eq 443
262 permit tcp 10.0.40.0 0.0.0.255 any eq ftp-data
263 permit tcp 10.0.40.0 0.0.0.255 any eq ftp
264 !
265 ipv6 route ::/0 2005:2013:FF:A0::2
266 !
267 !
268 !
269 ipv6 access-list ADMINv6
270 permit icmp any FF02::/16 router-solicitation
271 remark admin-dhcp
272 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
273 remark admin-dns

```

```

274 permit udp 2005:2013:FF:A20::/64 host 2005:2013:FF:A10::21 eq domain
275 remark admin-intsrv
276 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A10::/64
277 remark admin-int
278 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A30::/64
279 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A40::/64
280 remark admin-dmzsrv
281 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq www
282 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq 443
283 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq ftp-data
284 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq ftp
285 remark admin-dmzsrv-ftppasv
286 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 gt 48999
287 deny tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 gt 49999
288 remark admin-dmzsw
289 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::2 eq 22
290 remark admin-dmz-end
291 deny ipv6 2005:2013:FF:A20::/64 2005:2013:FF:B0::/64
292 remark admin-network
293 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A0::/64
294 remark admin-inet
295 permit tcp 2005:2013:FF:A20::/64 any
296 !
297 ipv6 access-list VERKAUFv6
298 permit icmp any FF02::/16 router-solicitation
299 remark verkauf-dhcp
300 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
301 remark verkauf-dns
302 permit udp 2005:2013:FF:A40::/64 host 2005:2013:FF:A10::21 eq domain
303 remark verkauf-intsrv
304 permit ipv6 2005:2013:FF:A40::/64 host 2005:2013:FF:A10::21
305 remark verkauf-intsrv-end
306 deny ipv6 2005:2013:FF:A40::/64 2005:2013:FF:A10::/64
307 remark verkauf-responddadmin
308 permit tcp 2005:2013:FF:A40::/64 2005:2013:FF:A20::/64 established
309 remark verkauf-dmzsrv
310 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq www
311 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq 443
312 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq ftp-data
313 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq ftp
314 remark verkauf-dmzsrv-ftppasv
315 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 gt 48999
316 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 lt 50000
317 remark verkauf-dmzsrv-end
318 deny ipv6 2005:2013:FF:A40::/64 2005:2013:FF:B0::/64
319 remark verkauf-inet
320 permit tcp 2005:2013:FF:A40::/64 any eq www
321 permit tcp 2005:2013:FF:A40::/64 any eq 443
322 permit tcp 2005:2013:FF:A40::/64 any eq ftp-data
323 permit tcp 2005:2013:FF:A40::/64 any eq ftp
324 !
325 ipv6 access-list DEVv6
326 permit icmp any FF02::/16 router-solicitation
327 remark dev-dhcp
328 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
329 remark dev-dns
330 permit udp 2005:2013:FF:A30::/64 host 2005:2013:FF:A10::21 eq domain
331 remark dev-intsrv
332 permit ipv6 2005:2013:FF:A30::/64 host 2005:2013:FF:A10::21
333 remark dev-intsrv-end
334 deny ipv6 2005:2013:FF:A30::/64 2005:2013:FF:A10::/64
335 remark dev-responddadmin
336 permit tcp 2005:2013:FF:A30::/64 2005:2013:FF:A20::/64 established
337 remark dev-dmzsrv
338 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq www
339 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq 443
340 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq ftp-data
341 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq ftp
342 remark dev-dmzsrv-ftppasv

```

```

343 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 gt 48999
344 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 lt 50000
345 remark dev-dmzsrv-end
346 deny ipv6 2005:2013:FF:A30::/64 2005:2013:FF:B0::/64
347 remark dev-inet
348 permit tcp 2005:2013:FF:A30::/64 any eq www
349 permit tcp 2005:2013:FF:A30::/64 any eq 443
350 permit tcp 2005:2013:FF:A30::/64 any eq ftp-data
351 permit tcp 2005:2013:FF:A30::/64 any eq ftp
352 !
353 ipv6 access-list INTSRVv6
354 remark intsrv-adm
355 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A20::/64 established
356 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A20::/64
357 permit udp 2005:2013:FF:A10::/64 eq 547 host 2005:2013:FF:A20::1 eq 547
358 remark intsrv-dev
359 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A30::/64 established
360 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A30::/64
361 permit udp 2005:2013:FF:A10::/64 eq 547 host 2005:2013:FF:A30::1 eq 547
362 remark intsrv-verkauf
363 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A40::/64 established
364 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A40::/64
365 remark intsrv-lan-end
366 deny ipv6 2005:2013:FF:A10::/64 2005:2013:FF:A00::/56
367 remark intsrv-dmzsrv
368 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq www
369 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq 443
370 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq ftp-data
371 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq ftp
372 remark admin-dmzsrv-ftppasv
373 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 gt 48999
374 deny tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 gt 49999
375 remark intsrv-dmzsrv-respond-radius
376 permit tcp host 2005:2013:FF:A10::21 eq 389 host 2005:2013:FF:B0::11 established
377 remark intsrv-dmzsrv-end
378 deny ipv6 2005:2013:FF:A10::/64 2005:2013:FF:B0::/64
379 remark intsrv-inet
380 permit tcp 2005:2013:FF:A10::/64 any eq www
381 permit tcp 2005:2013:FF:A10::/64 any eq 443
382 permit tcp 2005:2013:FF:A10::/64 any eq ftp-data
383 permit tcp 2005:2013:FF:A10::/64 any eq ftp
384 permit udp 2005:2013:FF:A10::/64 any eq domain
385 !
386 control-plane
387 !
388 !
389 !
390 !
391 mgcp behavior g729-variants static-pt
392 !
393 !
394 !
395 !
396 !
397 !
398 line con 0
399 exec-timeout 0 0
400 privilege level 15
401 logging synchronous
402 line aux 0
403 exec-timeout 0 0
404 privilege level 15
405 logging synchronous
406 line vty 0 4
407 login
408 !
409 !
410 end

```

B. Konfiguration ASA

```
1 : Saved
2 :
3 ASA Version 8.4(2)
4 !
5 hostname ciscoasa
6 enable password 8Ry2YjIyt7RRXU24 encrypted
7 passwd 2KFQnbNIdI.2KYOU encrypted
8 names
9 !
10 interface GigabitEthernet0
11   nameif outside
12   security-level 0
13   ip address 209.165.50.1 255.255.255.0
14   ipv6 address 2005:209:165:50::1/64
15   ipv6 enable
16 !
17 interface GigabitEthernet1
18   nameif dmz
19   security-level 50
20   ip address 172.16.0.1 255.255.255.0
21   ipv6 address 2005:2013:ff:b0::1/64
22   ipv6 enable
23 !
24 interface GigabitEthernet2
25   nameif inside
26   security-level 100
27   ip address 10.100.0.2 255.255.255.252
28   ipv6 address 2005:2013:ff:a0::2/64
29   ipv6 enable
30 !
31 interface GigabitEthernet3
32   shutdown
33   no nameif
34   no security-level
35   no ip address
36 !
37 interface GigabitEthernet4
38   shutdown
39   no nameif
40   no security-level
41   no ip address
42 !
43 interface GigabitEthernet5
44   shutdown
45   no nameif
46   no security-level
47   no ip address
48 !
49 ftp mode passive
50 object network NAT_inside_overload
51   subnet 10.0.0.0 255.255.0.0
52 object network NAT_dmzsrv_outside
53   host 209.165.50.2
54 object network NAT_dmz_static
55   host 172.16.0.21
56 object network NO_NAT_INSIDE
57   subnet 10.0.10.0 255.255.255.0
58 object network NO_NAT_VPN
59   subnet 10.0.99.0 255.255.255.0
60 object-group service dmzsrv2inet_UDPPorts udp
61   port-object eq domain
62 object-group service dmzsrv2inet_TCPSPorts tcp
63   port-object eq www
64   port-object eq https
65   port-object eq ftp-data
66   port-object eq ftp
```

```

67 object-group service inet2dmzsrv-TCPPorts tcp
68   port-object eq www
69   port-object eq https
70   port-object eq ftp-data
71   port-object eq ftp
72   port-object range 48999 49999
73 object-group network inside_subnets_ipv6
74   network-object 2005:2013:ff:a10::/64
75   network-object 2005:2013:ff:a20::/64
76   network-object 2005:2013:ff:a30::/64
77   network-object 2005:2013:ff:a40::/64
78   network-object 2005:2013:ff:a0::/64
79 access-list inside_in extended permit ip any any
80 access-list dmz_in remark dmzsrv-intsrv-ldap
81 access-list dmz_in extended permit tcp host 172.16.0.21 host 10.0.10.21 eq ldap
82 access-list dmz_in remark dmz-nolan-access
83 access-list dmz_in extended deny ip 172.16.0.0 255.255.255.0 10.0.0.0 255.0.0.0 log
84 access-list dmz_in remark dmzsrv-inet
85 access-list dmz_in extended permit tcp host 172.16.0.21 any object-group
    dmzsrv2inet-TCPPorts
86 access-list dmz_in extended permit udp host 172.16.0.21 any object-group
    dmzsrv2inet-UDPPorts
87 access-list dmz_in extended deny ip any any log
88 access-list outside_in remark wan-dmzsrv
89 access-list outside_in extended permit tcp any host 172.16.0.21 object-group
    inet2dmzsrv-TCPPorts
90 access-list outside_in extended deny ip any any log
91 access-list dmz extended permit ip any any
92 access-list 99 remark permit ip access from any to server subnet
93 access-list 99 extended permit ip any 10.0.10.0 255.255.255.0
94 access-list SPLIT-TUNNELLIST standard permit 10.0.10.0 255.255.255.0
95 pager lines 24
96 logging console informational
97 mtu outside 1500
98 mtu dmz 1500
99 mtu inside 1500
100 ip local pool VPN-ADMIN 10.0.99.1-10.0.99.126 mask 255.255.255.128
101 ip local pool VPN-USERS 10.0.99.129-10.0.99.254 mask 255.255.255.128
102 ipv6 icmp permit any dmz
103 ipv6 icmp permit any inside
104 ipv6 route inside 2005:2013:ff:a10::/64 2005:2013:ff:a0::1
105 ipv6 route inside 2005:2013:ff:a20::/64 2005:2013:ff:a0::1
106 ipv6 route inside 2005:2013:ff:a30::/64 2005:2013:ff:a0::1
107 ipv6 route inside 2005:2013:ff:a40::/64 2005:2013:ff:a0::1
108 ipv6 access-list dmz_in_v6 remark dmzsrv-intsrv-ldap
109 ipv6 access-list dmz_in_v6 permit tcp host 2005:2013:ff:b0::21 host
    2005:2013:ff:a10::21 eq ldap
110 ipv6 access-list dmz_in_v6 remark dmz-nolan-access
111 ipv6 access-list dmz_in_v6 deny ip 2005:2013:ff:b0::/64 object-group
    inside_subnets_ipv6
112 ipv6 access-list dmz_in_v6 remark dmzsrv-inet
113 ipv6 access-list dmz_in_v6 permit tcp host 2005:2013:ff:b0::21 any object-group
    dmzsrv2inet-TCPPorts
114 ipv6 access-list dmz_in_v6 permit udp host 2005:2013:ff:b0::21 any object-group
    dmzsrv2inet-UDPPorts
115 ipv6 access-list dmz_in_v6 deny ip any any log
116 ipv6 access-list outside_in_v6 remark wan-dmzsrv
117 ipv6 access-list outside_in_v6 permit tcp any host 2005:2013:ff:b0::21 object-group
    inet2dmzsrv-TCPPorts
118 ipv6 access-list outside_in_v6 deny ip any any log
119 ipv6 access-list inside_in_v6 permit ip any any
120 no failover
121 icmp unreachable rate-limit 1 burst-size 1
122 icmp deny any outside
123 icmp permit any dmz
124 icmp permit any inside
125 no asdm history enable
126 arp timeout 14400

```

```

127 nat (inside,outside) source static NO_NAT_INSIDE NO_NAT_INSIDE destination static
    NO_NAT_VPN NO_NAT_VPN
128 !
129 object network NAT_inside_overload
130 nat (inside,outside) dynamic interface
131 object network NAT_dmz_static
132 nat (dmz,outside) static NAT_dmzsrv_outside
133 access-group outside_in in interface outside
134 access-group outside_in_v6 in interface outside
135 access-group dmz_in in interface dmz
136 access-group dmz_in_v6 in interface dmz
137 access-group inside_in in interface inside
138 access-group inside_in_v6 in interface inside
139 route inside 10.0.0.0 255.255.0.0 10.100.0.1 1
140 timeout xlate 3:00:00
141 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
142 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
143 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
144 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
145 timeout tcp-proxy-reassembly 0:01:00
146 timeout floating-conn 0:00:00
147 dynamic-access-policy-record DfltAccessPolicy
148 user-identity default-domain LOCAL
149 aaa authentication ssh console LOCAL
150 no snmp-server location
151 no snmp-server contact
152 snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
153 crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
154 crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set ESP-3DES-SHA
155 crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000
156 crypto dynamic-map outside_dyn_map 10 set reverse-route
157 crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map
158 crypto map outside_map interface outside
159 crypto ikev1 enable outside
160 crypto ikev1 policy 65535
161 authentication pre-share
162 encryption aes-256
163 hash sha
164 group 2
165 lifetime 43200
166 telnet timeout 5
167 ssh 10.0.20.0 255.255.255.0 inside
168 ssh timeout 30
169 console timeout 0
170 threat-detection basic-threat
171 threat-detection statistics access-list
172 no threat-detection statistics tcp-intercept
173 group-policy VPN_ADMINISTRATOR internal
174 group-policy VPN_ADMINISTRATOR attributes
175 dns-server value 10.0.10.21
176 vpn-filter value 99
177 vpn-tunnel-protocol ikev1 ikev2
178 split-tunnel-policy tunnelspecified
179 split-tunnel-network-list value SPLIT_TUNNEL_LIST
180 default-domain value wosm.com
181 address-pools value VPN_ADMIN
182 group-policy VPN_USERS_GROUP internal
183 group-policy VPN_USERS_GROUP attributes
184 dns-server value 10.0.10.21
185 vpn-filter value 99
186 vpn-tunnel-protocol ikev1 ikev2
187 split-tunnel-policy tunnelspecified
188 split-tunnel-network-list value SPLIT_TUNNEL_LIST
189 default-domain value wosm.com
190 address-pools value VPN_USERS
191 username ssh_admin password SxYXLtULZ5hPDb07 encrypted privilege 15
192 username verkauf password FHPW9HqIN8QD22Y/ encrypted
193 username verkauf attributes
194 vpn-group-policy VPN_USERS_GROUP

```

```

195  vpn-filter value 99
196  username admin password f3UhLvUj1QsXsuK7 encrypted
197  username admin attributes
198  vpn-group-policy VPN_ADMINISTRATOR
199  vpn-filter value 99
200  tunnel-group VPN_ADMINISTRATOR type remote-access
201  tunnel-group VPN_ADMINISTRATOR general-attributes
202  address-pool VPN-ADMIN
203  default-group-policy VPN_ADMINISTRATOR
204  tunnel-group VPN_ADMINISTRATOR ipsec-attributes
205  ikev1 pre-shared-key *****
206  tunnel-group VPN_USERS.GROUP type remote-access
207  tunnel-group VPN_USERS.GROUP general-attributes
208  address-pool VPN-USERS
209  default-group-policy VPN_USERS.GROUP
210  tunnel-group VPN_USERS.GROUP ipsec-attributes
211  ikev1 pre-shared-key *****
212  !
213  !
214  prompt hostname context
215  no call-home reporting anonymous
216  call-home
217  profile CiscoTAC-1
218  no active
219  destination address http
220      https://tools.cisco.com/its/service/oddce/services/DDCEService
221  destination address email callhome@cisco.com
222  destination transport-method http
223  subscribe-to-alert-group diagnostic
224  subscribe-to-alert-group environment
225  subscribe-to-alert-group inventory periodic monthly
226  subscribe-to-alert-group configuration periodic monthly
227  subscribe-to-alert-group telemetry periodic daily
228  crashinfo save disable
229  Cryptochecksum:1a739f944de561e0353561d15a5f256e
230  : end

```