Workshop System Management

Tobias Lerch, Yanick Eberle, Pascal Schwarz

18. März 2013

Inhaltsverzeichnis

1. Netzwerk

1.1. Netzwerkdiagramm

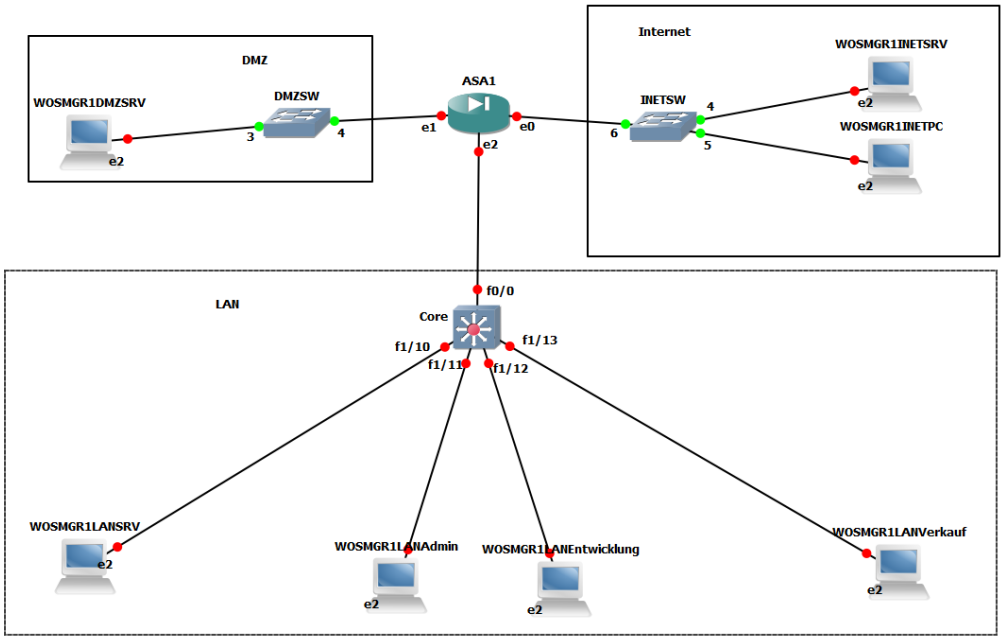

Abbildung 1: Netzwerk

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.

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 regulare 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 mitzueteilen, 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 Domänennamen. 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:

- Authenzifizierung: 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 gewähtleisten, 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 derInitiator 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 stürtzt 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-Flooging Attacken geschützt.

3.2. IP spoofing

3.2.1. Bedrohung

Ein Anfreifer sendet viele Anfragen an einen Server mit einer falschen Absender IP (z.B: 10.0.1.19). Dadurch wird der Server die Antworten zu den Anfragen an einen Client (10.0.1.19) senden. Der Server, sowie der Client wird dadurch ausgelastet.

3.2.2. Gegenmassnahme

Um sich gegen IP spoofing zu schützen, kann eine Überprüfung des 'Reverse-Path' aktiviert werden. So wird überprüft, ob die eingetragene Absenderadresse mit der effektiven Absenderadresse übereinstimmt.

3.3. ICMP 'smurf attack': Denial of Service

3.3.1. 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 so viele Echo Antworten dass der Server nicht mehr reagiert und abstürtzt.

3.3.2. Gegenmassnahme

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

3.4. Viren / Würmer / Trojaner

3.4.1. 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.

3.4.2. Gegenmassnahme

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

3.5. DNS Cache poisoning

3.5.1. 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.

3.5.2. Gegenmassnahme

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

3.6. Phishing

3.6.1. Bedrohung

Beim Phishing versucht ein Angreifer durch gefälschte Websiten, 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.

3.6.2. 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.

3.7. MAC flooding

3.7.1. 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 Packete jedem angeschlossenen Gerät. Nun kann der Angreifer jegliche Kommunikation über diesen Switch mithören.

3.7.2. 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.

3.8. ARP spoofing

3.8.1. 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.

3.8.2. 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.

3.9. Rogue DHCP

3.9.1. Bedrohung

Eine Person mit Zugriff auf ein Netzwerkkabel im internen Netz verbindet einen zusätzlichen, nicht autorisierten DHCP Server. Wenn der zusätzliche DHCP Sever 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 zugreiffen können.

3.9.2. 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.

3.10. 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	IP spoofing	ja
8	niedrig	mittel	MAC flooding	nein
9	niedrig	mittel	ARP spoofing	nein

3.11. Verteidigung gegen Attacken

3.11.1. ICMP 'smurf attack': Denial of Service

```
1  object-group service inet2dmzsrv_TCPPorts tcp
2   port-object eq www
3   port-object eq https
4   port-object eq ftp-data
5   port-object eq ftp
6   port-object range 48999 49999
7  !
8  access-list outside_in remark wan-dmzsrv
9  access-list outside_in extended permit tcp any host 172.16.0.21 object-group
       inet2dmzsrv_TCPPorts
10 access-list outside_in extended deny ip any any log
11 !
12 icmp deny any outside
```

3.11.2. TCP DoS (SYN-Flooding)

Folgende Policy Map schützt gegen SYN-Flooding:

```
1  policy-map tcpmap
2   class tcp_syn
3    set connection conn-max 100 embryonic-conn-max 100 per-client-max 10
         per-client-embryonic-max 10
4    set connection timeout embryonic 0:00:45 half-closed 0:05:00 idle 1:00:00
5  !
6  class-map tcp_syn
7   match any
```

3.11.3. IP spoofing

Folgender Befehl schützt gegen IP spoofing:

```
1 ip verify reverse-path interface outside
```

3.11.4. 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.

3.11.5. 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
```

```
 ip helper-address 10.0.10.21
 ipv6 address 2005:2013:FF:A40::1/64
 ipv6 traffic-filter VERKAUFv6 in
 ipv6 nd other-config-flag
 ipv6 dhcp relay destination 2005:2013:FF:A10::21
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.100.0.2
!
!
no ip http server
no ip http secure-server
!
ip access-list extended ADMIN
 remark admin-dhcp
 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
 remark admin-dns
 permit udp 10.0.20.0 0.0.0.255 host 10.0.10.21 eq domain
 remark admin-intsrv
 permit ip 10.0.20.0 0.0.0.255 10.0.10.0 0.0.0.255
 remark admin-int
 permit ip 10.0.20.0 0.0.0.255 10.0.30.0 0.0.0.255
 permit ip 10.0.20.0 0.0.0.255 10.0.40.0 0.0.0.255
 permit ip 10.0.20.0 0.0.0.255 10.0.99.0 0.0.0.255
 remark admin-dmzsrv
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq www
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq 443
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq ftp-data
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 eq ftp
 remark admin-dmzsrv-ftppasv
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 gt 48999
 deny   tcp 10.0.20.0 0.0.0.255 host 172.16.0.21 gt 49999
 remark admin-dmzsw
 permit tcp 10.0.20.0 0.0.0.255 host 172.16.0.2 eq 22
 remark admin-dmz-end
 deny   ip 10.0.20.0 0.0.0.255 172.16.0.0 0.0.0.255
 remark admin-network
 permit ip 10.0.20.0 0.0.0.255 10.0.100.0 0.0.0.255
 remark admin-inet
 permit tcp 10.0.20.0 0.0.0.255 any
ip access-list extended DEV
 remark dev-dhcp
 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
 remark dev-dns
 permit udp 10.0.30.0 0.0.0.255 host 10.0.10.21 eq domain
 remark dev-intsrv
 permit ip 10.0.30.0 0.0.0.255 host 10.0.10.21
 remark dev-intsrv-end
 deny   ip 10.0.30.0 0.0.0.255 10.0.10.0 0.0.0.255
 remark dev-respondadmin
 permit tcp 10.0.30.0 0.0.0.255 10.0.20.0 0.0.0.255 established
 remark dev-dmzsrv
 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq www
 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq 443
 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq ftp-data
 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 eq ftp
 remark dev-dmzsrv-ftppasv
 permit tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 gt 48999
 deny   tcp 10.0.30.0 0.0.0.255 host 172.16.0.21 gt 49999
 remark dev-dmzsrv-end
 deny   ip 10.0.30.0 0.0.0.255 172.16.0.0 0.0.0.255
 remark dev-inet
 permit tcp 10.0.30.0 0.0.0.255 any eq www
 permit tcp 10.0.30.0 0.0.0.255 any eq 443
 permit tcp 10.0.30.0 0.0.0.255 any eq ftp-data
 permit tcp 10.0.30.0 0.0.0.255 any eq ftp
ip access-list extended INTSRV
 remark intsrv-adm
 permit tcp 10.0.10.0 0.0.0.255 10.0.20.0 0.0.0.255 established
```

```
 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.20.0 0.0.0.255
 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.20.1 eq bootps
 remark intsrv-dev
 permit tcp 10.0.10.0 0.0.0.255 10.0.30.0 0.0.0.255 established
 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.30.0 0.0.0.255
 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.30.1 eq bootps
 remark intsrv-verkauf
 permit tcp 10.0.10.0 0.0.0.255 10.0.40.0 0.0.0.255 established
 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.40.0 0.0.0.255
 permit udp 10.0.10.0 0.0.0.255 eq bootps host 10.0.40.1 eq bootps
 remark intsrv-vpn
 permit tcp 10.0.10.0 0.0.0.255 10.0.99.0 0.0.0.255 established
 permit udp 10.0.10.0 0.0.0.255 eq domain 10.0.99.0 0.0.0.255
 remark intsrv-lan-end
 deny   ip 10.0.10.0 0.0.0.255 10.0.0.0 0.0.255.255
 remark intsrv-dmzsrv
 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq www
 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq 443
 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq ftp-data
 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 eq ftp
 remark admin-dmzsrv-ftppasv
 permit tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 gt 48999
 deny   tcp 10.0.10.0 0.0.0.255 host 172.16.0.21 gt 49999
 remark intsrv-dmzsrv-respond-radius
 permit tcp host 10.0.10.21 eq 389 host 172.16.0.21 established
 remark intsrv-dmzsrv-end
 deny   ip 10.0.10.0 0.0.0.255 172.16.0.0 0.0.0.255
 remark intsrv-inet
 permit tcp 10.0.10.0 0.0.0.255 any eq www
 permit tcp 10.0.10.0 0.0.0.255 any eq 443
 permit tcp 10.0.10.0 0.0.0.255 any eq ftp-data
 permit tcp 10.0.10.0 0.0.0.255 any eq ftp
 permit udp 10.0.10.0 0.0.0.255 any eq domain
ip access-list extended VERKAUF
 remark verkauf-dhcp
 permit udp host 0.0.0.0 eq bootpc host 255.255.255.255 eq bootps
 remark verkauf-dns
 permit udp 10.0.40.0 0.0.0.255 host 10.0.10.21 eq domain
 remark verkauf-intsrv
 permit ip 10.0.40.0 0.0.0.255 host 10.0.10.21
 remark verkauf-intsrv-end
 deny   ip 10.0.40.0 0.0.0.255 10.0.10.0 0.0.0.255
 remark verkauf-respondadmin
 permit tcp 10.0.40.0 0.0.0.255 10.0.20.0 0.0.0.255 established
 remark verkauf-dmzsrv
 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq www
 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq 443
 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq ftp-data
 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 eq ftp
 remark verkauf-dmzsrv-ftppasv
 permit tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 gt 48999
 deny   tcp 10.0.40.0 0.0.0.255 host 172.16.0.21 gt 49999
 remark verkauf-dmzsrv-end
 deny   ip 10.0.40.0 0.0.0.255 172.16.0.0 0.0.0.255
 remark verkauf-inet
 permit tcp 10.0.40.0 0.0.0.255 any eq www
 permit tcp 10.0.40.0 0.0.0.255 any eq 443
 permit tcp 10.0.40.0 0.0.0.255 any eq ftp-data
 permit tcp 10.0.40.0 0.0.0.255 any eq ftp
!
ipv6 route ::/0 2005:2013:FF:A0::2
!
!
!
ipv6 access-list ADMINv6
 permit icmp any FF02::/16 router-solicitation
 remark admin-dhcp
 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
 remark admin-dns
```

```
 permit udp 2005:2013:FF:A20::/64 host 2005:2013:FF:A10::21 eq domain
 remark admin-intsrv
 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A10::/64
 remark admin-int
 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A30::/64
 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A40::/64
 remark admin-dmzsrv
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq www
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq 443
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq ftp-data
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 eq ftp
 remark admin-dmzsrv-ftppasv
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 gt 48999
 deny tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::21 gt 49999
 remark admin-dmzsw
 permit tcp 2005:2013:FF:A20::/64 host 2005:2013:FF:B0::2 eq 22
 remark admin-dmz-end
 deny ipv6 2005:2013:FF:A20::/64 2005:2013:FF:B0::/64
 remark admin-network
 permit ipv6 2005:2013:FF:A20::/64 2005:2013:FF:A0::/64
 remark admin-inet
 permit tcp 2005:2013:FF:A20::/64 any
!
ipv6 access-list VERKAUFv6
 permit icmp any FF02::/16 router-solicitation
 remark verkauf-dhcp
 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
 remark verkauf-dns
 permit udp 2005:2013:FF:A40::/64 host 2005:2013:FF:A10::21 eq domain
 remark verkauf-intsrv
 permit ipv6 2005:2013:FF:A40::/64 host 2005:2013:FF:A10::21
 remark verkauf-intsrv-end
 deny ipv6 2005:2013:FF:A40::/64 2005:2013:FF:A10::/64
 remark verkauf-respondadmin
 permit tcp 2005:2013:FF:A40::/64 2005:2013:FF:A20::/64 established
 remark verkauf-dmzsrv
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq www
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq 443
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq ftp-data
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 eq ftp
 remark verkauf-dmzsrv-ftppasv
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 gt 48999
 permit tcp 2005:2013:FF:A40::/64 host 2005:2013:FF:B0::21 lt 50000
 remark verkauf-dmzsrv-end
 deny ipv6 2005:2013:FF:A40::/64 2005:2013:FF:B0::/64
 remark verkauf-inet
 permit tcp 2005:2013:FF:A40::/64 any eq www
 permit tcp 2005:2013:FF:A40::/64 any eq 443
 permit tcp 2005:2013:FF:A40::/64 any eq ftp-data
 permit tcp 2005:2013:FF:A40::/64 any eq ftp
!
ipv6 access-list DEVv6
 permit icmp any FF02::/16 router-solicitation
 remark dev-dhcp
 permit udp FE80::/16 eq 546 host FF02::1:2 eq 547
 remark dev-dns
 permit udp 2005:2013:FF:A30::/64 host 2005:2013:FF:A10::21 eq domain
 remark dev-intsrv
 permit ipv6 2005:2013:FF:A30::/64 host 2005:2013:FF:A10::21
 remark dev-intsrv-end
 deny ipv6 2005:2013:FF:A30::/64 2005:2013:FF:A10::/64
 remark dev-respondadmin
 permit tcp 2005:2013:FF:A30::/64 2005:2013:FF:A20::/64 established
 remark dev-dmzsrv
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq www
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq 443
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq ftp-data
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 eq ftp
 remark dev-dmzsrv-ftppasv
```

```
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 gt 48999
 permit tcp 2005:2013:FF:A30::/64 host 2005:2013:FF:B0::21 lt 50000
 remark dev-dmzsrv-end
 deny ipv6 2005:2013:FF:A30::/64 2005:2013:FF:B0::/64
 remark dev-inet
 permit tcp 2005:2013:FF:A30::/64 any eq www
 permit tcp 2005:2013:FF:A30::/64 any eq 443
 permit tcp 2005:2013:FF:A30::/64 any eq ftp-data
 permit tcp 2005:2013:FF:A30::/64 any eq ftp
!
ipv6 access-list INTSRVv6
 remark intsrv-adm
 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A20::/64 established
 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A20::/64
 permit udp 2005:2013:FF:A10::/64 eq 547 host 2005:2013:FF:A20::1 eq 547
 remark intsrv-dev
 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A30::/64 established
 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A30::/64
 permit udp 2005:2013:FF:A10::/64 eq 547 host 2005:2013:FF:A30::1 eq 547
 remark intsrv-verkauf
 permit tcp 2005:2013:FF:A10::/64 2005:2013:FF:A40::/64 established
 permit udp 2005:2013:FF:A10::/64 eq domain 2005:2013:FF:A40::/64
 remark intsrv-lan-end
 deny ipv6 2005:2013:FF:A10::/64 2005:2013:FF:A00::/56
 remark intsrv-dmzsrv
 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq www
 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq 443
 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq ftp-data
 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 eq ftp
 remark admin-dmzsrv-ftppasv
 permit tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 gt 48999
 deny tcp 2005:2013:FF:A10::/64 host 2005:2013:FF:B0::21 gt 49999
 remark intsrv-dmzsrv-respond-radius
 permit tcp host 2005:2013:FF:A10::21 eq 389 host 2005:2013:FF:B0::11 established
 remark intsrv-dmzsrv-end
 deny ipv6 2005:2013:FF:A10::/64 2005:2013:FF:B0::/64
 remark intsrv-inet
 permit tcp 2005:2013:FF:A10::/64 any eq www
 permit tcp 2005:2013:FF:A10::/64 any eq 443
 permit tcp 2005:2013:FF:A10::/64 any eq ftp-data
 permit tcp 2005:2013:FF:A10::/64 any eq ftp
 permit udp 2005:2013:FF:A10::/64 any eq domain
!
control-plane
!
!
!
!
mgcp behavior g729-variants static-pt
!
!
!
!
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
line vty 0 4
 login
!
!
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_TCPPorts tcp
63  port-object eq www
64  port-object eq https
65  port-object eq ftp-data
66  port-object eq ftp
```

```
object-group service inet2dmzsrv_TCPPorts tcp
 port-object eq www
 port-object eq https
 port-object eq ftp-data
 port-object eq ftp
 port-object range 48999 49999
object-group network inside_subnets_ipv6
 network-object 2005:2013:ff:a10::/64
 network-object 2005:2013:ff:a20::/64
 network-object 2005:2013:ff:a30::/64
 network-object 2005:2013:ff:a40::/64
 network-object 2005:2013:ff:a0::/64
access-list inside_in extended permit ip any any
access-list dmz_in remark dmzsrv-intsrv_ldap
access-list dmz_in extended permit tcp host 172.16.0.21 host 10.0.10.21 eq ldap
access-list dmz_in remark dmz-nolan-access
access-list dmz_in extended deny ip 172.16.0.0 255.255.255.0 10.0.0.0 255.0.0.0 log
access-list dmz_in remark dmzsrv-inet
access-list dmz_in extended permit tcp host 172.16.0.21 any object-group
    dmzsrv2inet_TCPPorts
access-list dmz_in extended permit udp host 172.16.0.21 any object-group
    dmzsrv2inet_UDPPorts
access-list dmz_in extended deny ip any any log
access-list outside_in remark wan-dmzsrv
access-list outside_in extended permit tcp any host 172.16.0.21 object-group
    inet2dmzsrv_TCPPorts
access-list outside_in extended deny ip any any log
access-list dmz extended permit ip any any
access-list 99 remark permit ip access from any to server subnet
access-list 99 extended permit ip any 10.0.10.0 255.255.255.0
access-list SPLIT_TUNNEL_LIST standard permit 10.0.10.0 255.255.255.0
pager lines 24
logging console informational
mtu outside 1500
mtu dmz 1500
mtu inside 1500
ip local pool VPN-ADMIN 10.0.99.1-10.0.99.126 mask 255.255.255.128
ip local pool VPN-USERS 10.0.99.129-10.0.99.254 mask 255.255.255.128
ip verify reverse-path interface outside
ipv6 icmp deny any outside
ipv6 icmp permit any dmz
ipv6 icmp permit any inside
ipv6 route inside 2005:2013:ff:a10::/64 2005:2013:ff:a0::1
ipv6 route inside 2005:2013:ff:a20::/64 2005:2013:ff:a0::1
ipv6 route inside 2005:2013:ff:a30::/64 2005:2013:ff:a0::1
ipv6 route inside 2005:2013:ff:a40::/64 2005:2013:ff:a0::1
ipv6 access-list dmz_in_v6 remark dmzsrv-intsrv_ldap
ipv6 access-list dmz_in_v6 permit tcp host 2005:2013:ff:b0::21 host
    2005:2013:ff:a10::21 eq ldap
ipv6 access-list dmz_in_v6 remark dmz-nolan-access
ipv6 access-list dmz_in_v6 deny ip 2005:2013:ff:b0::/64 object-group
    inside_subnets_ipv6
ipv6 access-list dmz_in_v6 remark dmzsrv-inet
ipv6 access-list dmz_in_v6 permit tcp host 2005:2013:ff:b0::21 any object-group
    dmzsrv2inet_TCPPorts
ipv6 access-list dmz_in_v6 permit udp host 2005:2013:ff:b0::21 any object-group
    dmzsrv2inet_UDPPorts
ipv6 access-list dmz_in_v6 deny ip any any log
ipv6 access-list outside_in_v6 remark  wan-dmzsrv
ipv6 access-list outside_in_v6 permit tcp any host 2005:2013:ff:b0::21 object-group
    inet2dmzsrv_TCPPorts
ipv6 access-list outside_in_v6 deny ip any any log
ipv6 access-list inside_in_v6 permit ip any any
no failover
icmp unreachable rate-limit 1 burst-size 1
icmp deny any outside
icmp permit any dmz
icmp permit any inside
no asdm history enable
```

```
128 arp timeout 14400
129 nat (inside,outside) source static NO_NAT_INSIDE NO_NAT_INSIDE destination static
        NO_NAT_VPN NO_NAT_VPN
130 !
131 object network NAT_inside_overload
132  nat (inside,outside) dynamic interface
133 object network NAT_dmz_static
134  nat (dmz,outside) static NAT_dmzsrv_outside
135 access-group outside_in in interface outside
136 access-group outside_in_v6 in interface outside
137 access-group dmz_in in interface dmz
138 access-group dmz_in_v6 in interface dmz
139 access-group inside_in in interface inside
140 access-group inside_in_v6 in interface inside
141 route inside 10.0.0.0 255.255.0.0 10.100.0.1 1
142 timeout xlate 3:00:00
143 timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
144 timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
145 timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
146 timeout sip-provisional-media 0:02:00 uauth 0:05:00 absolute
147 timeout tcp-proxy-reassembly 0:01:00
148 timeout floating-conn 0:00:00
149 dynamic-access-policy-record DfltAccessPolicy
150 user-identity default-domain LOCAL
151 aaa authentication ssh console LOCAL
152 no snmp-server location
153 no snmp-server contact
154 snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart
155 crypto ipsec ikev1 transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
156 crypto dynamic-map outside_dyn_map 10 set ikev1 transform-set ESP-3DES-SHA
157 crypto dynamic-map outside_dyn_map 10 set security-association lifetime seconds 288000
158 crypto dynamic-map outside_dyn_map 10 set reverse-route
159 crypto map outside_map 10 ipsec-isakmp dynamic outside_dyn_map
160 crypto map outside_map interface outside
161 crypto ikev1 enable outside
162 crypto ikev1 policy 65535
163  authentication pre-share
164  encryption aes-256
165  hash sha
166  group 2
167  lifetime 43200
168 telnet timeout 5
169 ssh 10.0.20.0 255.255.255.0 inside
170 ssh timeout 30
171 console timeout 0
172 threat-detection basic-threat
173 threat-detection statistics access-list
174 threat-detection statistics tcp-intercept rate-interval 30 burst-rate 400
        average-rate 200
175 group-policy VPN_ADMINISTRATOR internal
176 group-policy VPN_ADMINISTRATOR attributes
177  dns-server value 10.0.10.21
178  vpn-filter value 99
179  vpn-tunnel-protocol ikev1 ikev2
180  split-tunnel-policy tunnelspecified
181  split-tunnel-network-list value SPLIT_TUNNEL_LIST
182  default-domain value wosm.com
183  address-pools value VPN-ADMIN
184 group-policy VPN_USERS_GROUP internal
185 group-policy VPN_USERS_GROUP attributes
186  dns-server value 10.0.10.21
187  vpn-filter value 99
188  vpn-tunnel-protocol ikev1 ikev2
189  split-tunnel-policy tunnelspecified
190  split-tunnel-network-list value SPLIT_TUNNEL_LIST
191  default-domain value wosm.com
192  address-pools value VPN-USERS
193 username ssh_admin password SxYXLtULZ5hPDb07 encrypted privilege 15
194 username verkauf password FHPW9HqlN8QD22Y/ encrypted
```

```
195 username verkauf attributes
196  vpn-group-policy VPN_USERS_GROUP
197  vpn-filter value 99
198 username admin password f3UhLvUj1QsXsuK7 encrypted
199 username admin attributes
200  vpn-group-policy VPN_ADMINISTRATOR
201  vpn-filter value 99
202 tunnel-group VPN_ADMINISTRATOR type remote-access
203 tunnel-group VPN_ADMINISTRATOR general-attributes
204  address-pool VPN-ADMIN
205  default-group-policy VPN_ADMINISTRATOR
206 tunnel-group VPN_ADMINISTRATOR ipsec-attributes
207  ikev1 pre-shared-key *****
208 tunnel-group VPN_USERS_GROUP type remote-access
209 tunnel-group VPN_USERS_GROUP general-attributes
210  address-pool VPN-USERS
211  default-group-policy VPN_USERS_GROUP
212 tunnel-group VPN_USERS_GROUP ipsec-attributes
213  ikev1 pre-shared-key *****
214 !
215 class-map tcp_syn
216  match any
217 class-map inspection_default
218  match default-inspection-traffic
219 !
220 !
221 policy-map type inspect dns preset_dns_map
222  parameters
223   message-length maximum 512
224 policy-map global_policy
225  class inspection_default
226   inspect dns preset_dns_map
227   inspect ftp
228   inspect h323 h225
229   inspect h323 ras
230   inspect rsh
231   inspect rtsp
232   inspect esmtp
233   inspect sqlnet
234   inspect skinny
235   inspect sunrpc
236   inspect xdmcp
237   inspect sip
238   inspect netbios
239   inspect tftp
240   inspect http
241 policy-map tcpmap
242  class tcp_syn
243   set connection conn-max 100 embryonic-conn-max 100 per-client-max 10
        per-client-embryonic-max 10
244   set connection timeout embryonic 0:00:45 half-closed 0:05:00 idle 1:00:00
245 !
246 service-policy tcpmap global
247 service-policy global_policy interface outside
248 prompt hostname context
249 no call-home reporting anonymous
250 call-home
251  profile CiscoTAC-1
252   no active
253   destination address http
        https://tools.cisco.com/its/service/oddce/services/DDCEService
254   destination address email callhome@cisco.com
255   destination transport-method http
256   subscribe-to-alert-group diagnostic
257   subscribe-to-alert-group environment
258   subscribe-to-alert-group inventory periodic monthly
259   subscribe-to-alert-group configuration periodic monthly
260   subscribe-to-alert-group telemetry periodic daily
261 crashinfo save disable
```

```
262  Cryptochecksum:95fef6474f36e5fb331ab197685106b8
263  : end
```