|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Template "Härtungsempfehlungen für Cisco IOS und NX-OS"

3. Juni 2022

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | TMP400011 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung (vergeben] |
| Name des Dokuments | Template "Härtungsempfehlungen für Cisco IOS und NX-OS" | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 5 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc114910295)

[Dokumentenhistorie 3](#_Toc114910296)

[Inhaltsverzeichnis 4](#_Toc114910297)

[1 Empfehlungen für IOS-basierte Systeme 8](#_Toc114910298)

[1.1 Allgemeine Vorgaben 8](#_Toc114910299)

[1.2 NTP 8](#_Toc114910300)

[1.3 Zeitzone und automatische Umschaltung 8](#_Toc114910301)

[1.4 Erforderliche Service 8](#_Toc114910302)

[1.5 Nicht unbedingt erforderliche Service und Funktionen 9](#_Toc114910303)

[1.6 Nicht empfohlener Service bei sehr hohem Schutzbedarf 9](#_Toc114910304)

[1.7 DNS und Hostnamen 9](#_Toc114910305)

[1.8 Management-Interface 10](#_Toc114910306)

[1.9 SSH-Server 10](#_Toc114910307)

[1.10 Lokale Benutzer und Tacacs+ 11](#_Toc114910308)

[1.11 Terminal (VTY) – Filterliste (ACL) 13](#_Toc114910309)

[1.12 Terminal (VTY) – Konsolen-Port 14](#_Toc114910310)

[1.13 Monitoring und Reporting 14](#_Toc114910311)

[1.14 Spanning-Tree 16](#_Toc114910312)

[1.15 Netflow 16](#_Toc114910313)

[1.16 VLAN Trunking Protocol (VTP) 17](#_Toc114910314)

[1.17 Nicht genutzte Ports aus dem Default-VLAN entfernen 17](#_Toc114910315)

[1.18 Aktivieren von Port-Security zum Schutze vor MAC-Flooding 17](#_Toc114910316)

[1.19 Traffic Storm Control 17](#_Toc114910317)

[1.20 Konfiguration des EtherChannel 18](#_Toc114910318)

[1.21 Konfiguration des Trunk-Ports 18](#_Toc114910319)

[2 Empfehlungen für NX-OS-basierte Systeme 20](#_Toc114910320)

[2.1 NTP 20](#_Toc114910321)

[2.2 Zeitzone und automatische Umschaltung 20](#_Toc114910322)

[2.3 Lokale Benutzer und TACACS+ 20](#_Toc114910323)

[2.4 Telnet-Server 21](#_Toc114910324)

[2.5 SSH-Server 21](#_Toc114910325)

[2.6 Terminal (VTY)-Filterliste 21](#_Toc114910326)

[2.7 Terminal (VTY) Console-Ports 22](#_Toc114910327)

[2.8 Monitoring und Reporting (only snmp) 22](#_Toc114910328)

[2.9 Spanning-Tree anpassen 23](#_Toc114910329)

[2.10 NetFlow 23](#_Toc114910330)

[2.11 VLAN Trunking Protocol (VTP) 24](#_Toc114910331)

[2.12 Nicht genutzte Ports aus dem Default-VLAN entfernen 24](#_Toc114910332)

[2.13 Aktivieren von Port-Security zum Schutze vor MAC-Flooding 24](#_Toc114910333)

Abkürzungsverzeichnis

Siehe Anlage zentrales Abkürzungsverzeichnis Informationssicherheit.

Abbildungsverzeichnis

**Es konnten keine Einträge für ein Abbildungsverzeichnis gefunden werden.**

Tabellenverzeichnis

[Tabelle 1: IOS-basierte Systeme- allgemeine Vorgaben 8](#_Toc114910334)

[Tabelle 2: IOS-basierte Systeme - NTP Vorgaben 8](#_Toc114910335)

[Tabelle 3: IOS-basierte Systeme - Zeitzone und automatische Umschaltung 8](#_Toc114910336)

[Tabelle 4: IOS-basierte Systeme - benötigte Services 9](#_Toc114910337)

[Tabelle 5: IOS-basierte System – nicht benötigte Services und Funktionen 9](#_Toc114910338)

[Tabelle 6: IOS-basierte System – nicht benötigte Services bei sehr hohem Schutzbedarf 9](#_Toc114910339)

[Tabelle 7: IOS-basierte System – DNS und Hostname 9](#_Toc114910340)

[Tabelle 8: IOS-basierte System – Management-Interface 10](#_Toc114910341)

[Tabelle 9: IOS-basierte System – SSH-Server 10](#_Toc114910342)

[Tabelle 10: IOS-basierte System – lokale Benutzer und TACACS+ 13](#_Toc114910343)

[Tabelle 11: IOS-basierte Systeme – VTY-Filterliste 13](#_Toc114910344)

[Tabelle 12: IOS-basierte System – VTY und Konsolen-Port 14](#_Toc114910345)

[Tabelle 13: IOS-basierte Systeme – Monitoring und Reporting 15](#_Toc114910346)

[Tabelle 14: IOS-basierte System – Spanning-Tree 16](#_Toc114910347)

[Tabelle 15: IOS-basierte System – Netflow 16](#_Toc114910348)

[Tabelle 16: IOS-basierte System – VLAN Trunking Protocol (VTP) 17](#_Toc114910349)

[Tabelle 17: IOS-basierte System – verschieben der nicht genutzten Ports 17](#_Toc114910350)

[Tabelle 18: IOS-basierte Systeme – Aktivieren von Port-Security zum Schutze vor MAC-Flooding 17](#_Toc114910351)

[Tabelle 19: IOS-basierte Systeme – Traffic Storm Control 17](#_Toc114910352)

[Tabelle 20: IOS-basierte System – Konfiguration EtherChannel 18](#_Toc114910353)

[Tabelle 21: IOS-basierte System – Konfiguration des Trunk-Ports 19](#_Toc114910354)

[Tabelle 22: NX-OS-basierte System - NTP Vorgaben 20](#_Toc114910355)

[Tabelle 23: NX-OS-basierte System - Zeitzone und automatische Umschaltung 20](#_Toc114910356)

[Tabelle 24: NX-OS-basierte System – lokale Benutzer und TACACS+ 21](#_Toc114910357)

[Tabelle 25: NX-OS-basierte System – Telnet-Server 21](#_Toc114910358)

[Tabelle 26: NX-OS-basierte System – SSH-Server 21](#_Toc114910359)

[Tabelle 27: NX-OS-basierte System – VTY-Filterliste 21](#_Toc114910360)

[Tabelle 28: NX-OS-basierte System – VTY und Console 22](#_Toc114910361)

[Tabelle 29: NX-OS-basierte System – Monitoring und Reporting 22](#_Toc114910362)

[Tabelle 30: IOS-basierte System – Spanning-Tree anpassen 23](#_Toc114910363)

[Tabelle 31: NX-OS-basierte System – Netflow 23](#_Toc114910364)

[Tabelle 32: NX-OS-basierte System – VLAN Trunking Protocol (VTP) 24](#_Toc114910365)

[Tabelle 33: NX-OS-basierte System – verschieben der nicht genutzten Ports 24](#_Toc114910366)

[Tabelle 34: NX-OS-basierte System – Aktivieren von Port-Security zum Schutze vor MAC-Flooding 24](#_Toc114910367)

# Empfehlungen für IOS-basierte Systeme

## Allgemeine Vorgaben

|  |  |
| --- | --- |
| **Beschreibung** | **Befehl - Feldname** |
| Boot-System-Kommando | boot-start-marker  boot system <speicherort>:<ios-filename>  boot-end-marker |
| Aktivieren der geschützten Ablage der IOS und der Konfiguration | secure boot-image  secure boot−config |

Tabelle 1: IOS-basierte Systeme- allgemeine Vorgaben

## NTP

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegung der NTP Parameter und des max. 8-stelligen Hashes zur Authentisierung | ntp authenticate  ntp authentication-key <key-id> md5 <hash>  ntp trusted-key <key-id>  ntp maxdistance 1  ntp broadcastdelay 0  ntp peer <peer\_address> key <key-id>  ntp server <server\_address> key <key-id> |

Tabelle 2: IOS-basierte Systeme - NTP Vorgaben

## Zeitzone und automatische Umschaltung

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| MET ist die Zeitzone und automatisches Umschalten zwischen Winter und Sommerzeit soll aktiviert werden | clock timezone CET 1 0  clock summer-time CEST recurring last Sun Mar 2:00 last Sun Oct 3:00 |

Tabelle 3: IOS-basierte Systeme - Zeitzone und automatische Umschaltung

## Erforderliche Service

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Debug und Syslog enthält Zeitstempel nach lokaler Zeitzone. Passwörter werden nur verschlüsselt abgelegt. Statistiken werden alle 5s erhoben. | service timestamps debug datetime localtime show-timezone  service timestamps log datetime localtime show-timezone  service password-encryption  service counters max age 5 |

Tabelle 4: IOS-basierte Systeme - benötigte Services

## Nicht unbedingt erforderliche Service und Funktionen

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Nicht benötigte Services werden abgeschaltet. | no service tcp-keepalives-in  no service tcp-keepalives-out  no service pad  no service config  no service nagle  no service call-home |
| Nicht benötigte Funktionen werden deaktiviert | no ip finger  no ip bootp server  ip dhcp bootp ignore  no ip domain-lookup  no ip http server  no ip http secure-server  no cdp run  no lldp run  no ip source-route  no ip gratuitous-arps |

Tabelle 5: IOS-basierte System – nicht benötigte Services und Funktionen

## Nicht empfohlener Service bei sehr hohem Schutzbedarf

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| nicht benötigter Servic bei sehr hohem Schutzbedarf oder ungenügender physikalischer Absicherung des Switches. | no service password-recovery |

Tabelle 6: IOS-basierte System – nicht benötigte Services bei sehr hohem Schutzbedarf

## DNS und Hostnamen

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegung Hostname und Domain | hostname <hostname>  ip domain-name <domain-name> |

Tabelle 7: IOS-basierte System – DNS und Hostname

## Management-Interface

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Einrichten eines Management-Interfaces mittels Interface-VLAN | VLAN<VLAN-ID-Mng>  name <management-interface>  mac address-table aging-time 36000 vlan <VLAN-ID-Mng>  !  interface vlan <VLAN-ID-Mng>  description +++ <management-interface> +++  ip address <Mng\_IP-Adresse> <mask>  no shutdown |
| Einrichten eines Management-Interfaces mittels GigabitEthernet-Interface | interface GigabitEthernet<ID>/<ID>  description +++ <management-interface> +++  switchport  switchport access vlan <VLAN-ID-Mng>  no shutdown  !  interface vlan <VLAN-ID-Mng>  description +++ <management-interface> +++  ip address <Mng\_IP-Adresse> <mask>  no shutdown |
| Einrichten der Management-Default-Route | ip default-gateway <next hop> |

Tabelle 8: IOS-basierte System – Management-Interface

## SSH-Server

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegen der SSH-Server-Version sowie Umsetzung von Härtungsmaßnahmen | crypto key generate rsa modulus 2048  ip ssh version 2  ip ssh dh min size 2048  ip ssh time-out 60  ip ssh stricthostkeycheck  ip ssh server algorithm encryption aes256-ctr  ip ssh server algorithm mac hmac-sha1  ip ssh authentication-retries 3  ip scp server enable  ip ssh source−interface <Mng-Interface> |

Tabelle 9: IOS-basierte System – SSH-Server

## Lokale Benutzer und Tacacs+

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Aktivieren der Passwort-Richtlinie | security passwords min-length <Länge größer 12 Zeichen> |
| Lokale Nutzer für Notfallzugriff | username <notfallbenutzer> secret <Passwort> |
| Anzahl der Anmeldeversuche | security authentication failure rate 5 log |
| Festlegen der IP-Adressen des TACACS-Servers für die Authentisierung. | aaa group server tacacs+ <TACACS-GROUP>  server-private <1. TACACS-IP-Add> key <Passwort>  server-private <2. TACACS-IP-Add> key <Passwort>  ip tacacs source-interface <Interface>  !  aaa authentication login default group <TACACS-GROUP> local  aaa authentication login console group <TACACS-GROUP> local  aaa authentication login <TACACS-GROUP> group tacacs+ local  aaa authorization console  aaa authorization exec default group <TACACS-GROUP> local  aaa authorization exec console group <TACACS-GROUP> local  aaa accounting exec default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 1 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 2 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 3 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 4 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 5 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 6 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting connection default  action-type start-stop  group <TACACS-GROUP>  aaa accounting system default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 7 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 8 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 9 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 10 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 11 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 12 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 13 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 14 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting commands 15 default  action-type start-stop  group <TACACS-GROUP>  aaa accounting network default  action-type start-stop  group <TACACS-GROUP> |
| Setzen der DoS-Erkennungsparameter | login block-for 10 attempts 3 within 10 |
| Anlegen des Passwortes für Level15 | enable secret <Passwort> |

Tabelle 10: IOS-basierte System – lokale Benutzer und TACACS+

## Terminal (VTY) – Filterliste (ACL)

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Erstellen der VTY-Filterliste | ip access-list standard <VTY-ACL-Name>  permit <IP-Adresse>  permit <IP-Netz> <Netz-Maske>  deny any log |

Tabelle 11: IOS-basierte Systeme – VTY-Filterliste

## Terminal (VTY) – Konsolen-Port

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegen der Authentifizierung für den Konsolzugriff. Die Authentifizierung erfolgt über TACACS+, wenn dieser nicht erreichbar ist, wird über den lokalen Nutzer authentifiziert | line con 0  session-timeout 20  exec-timeout 20 0  authorization exec console  logging synchronous  login authentication console |
| Terminal (VTY) -Zugriff auf Komponenten. Es wird nur SSH zugelassen | line vty 0 4  session-timeout 20  exec-timeout 20 0  logging synchronous  history size 40  transport input ssh  access-class ssh in |
| Hiermit werden die VTY-Zugänge Nr. 5 bis 15 deaktiviert. | line vty 5 15  session-timeout 20  exec-timeout 20 0  logging synchronous  history size 40  transport input ssh  access-class ssh in |

Tabelle 12: IOS-basierte System – VTY und Konsolen-Port

## Monitoring und Reporting

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| SNMP-Parameter zur Identifizierung des Systems im Monitoring festlegen | snmp-server ifindex persist  snmp-server location <Ort>, <Gebäude>, <Raum-Nr.>, <Datenschrank>  snmp-server contact <Nummer>,<Name>snmp-server chassis-id <„sh snmp chassis“> |
| Filter-Liste zum Eingrenzen der erlaubten IP-Adressen für den lesenden Zugriff | ip access-list standard <snmp-RO>  remark Dienstleister  permit <IP-Netz> <Netz-Maske> |
| Filter-Liste zum Eingrenzen der erlaubten IP-Adressen für den schreibenden Zugriff | ip access-list standard <snmp-RW>  remark NMC  permit <IP-Netz> <Netz-Maske>  remark Mng-Tool  permit <IP-Netz> <Netz-Maske> |
| SNMP-Parameter für den lesenden Zugriff festlegen. | snmp-server user <read-group> <read-group> v3 auth sha <PASSWORD> priv aes 256 <PRIV-PASSWORD> access <snmp-RO>  snmp-server group <read-group> v3 priv read <read-view> access <snmp-RO>  snmp-server view <read-view> internet included |
| SNMP-Parameter für den schreibenden Zugriff festlegen. | snmp-server user <write-group> <write-group> v3 auth sha <PASSWORD> priv aes 256 <PRIV-PASSWORD> access snmp-RW  snmp-server group <write-group> v3 priv read <write-view> access <snmp-RW>  snmp-server view <write-view> system included |
| Trapziele festlegen und Traps erlauben. Für jeden Trap-Server wird eine IP-Adresse eingetragen. Das Source-Interface ist anzupassen. | snmp-server user <TRAP> <TRAP> v3 auth sha <PASSWORD> priv aes 256 <PRIV-PASSWORD>  snmp-server group <TRAP> v3 priv  snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart  snmp-server enable traps tty  snmp-server enable traps cpu threshold  snmp-server enable traps port-security  snmp-server enable traps storm-control trap-rate 0  snmp-server enable traps envmon fan shutdown supply temperature status  snmp-server host <IP snmp-server host> version 3 priv TRAP |
| Festlegen der Logging Parameter. | logging origin-id string <Wert>  no logging console  logging buffered 512000  logging trap debugging  logging facility local6  logging host <IP-Adresse1>  logging host <IP-Adresse2>  logging event link-status default  logging source-interface <Mng-Interface> |
| Aktivieren des Tracken von Konfigurationsänderungen und versenden an zentralen Server via Secure Copy | archive  log config  logging enable  hidekeys  path scp://<scp\_Benutzer>:<scp-Passwort>@<Server-IP>/$h  write-memory |

Tabelle 13: IOS-basierte Systeme – Monitoring und Reporting

## Spanning-Tree

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| alle Access-Ports von der SPT-Root-Elektion ausschließen | interface range gigabitethernet <slot>/<start-interface> - <end-interface>  spanning-tree portfast |
| Alle Access-Ports die ein BPDU-Paket empfangen sollen abgeschaltet werden | spanning-tree portfast bpduguard |

Tabelle 14: IOS-basierte System – Spanning-Tree

## Netflow

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Konfiguration des Netflow Exporter | flow exporter <flow exporter name>  destination <IP-address from flow-collector> |
| Konfiguration des Netflow Records | flow record <flow record name>  match ipv4 dscp  match ipv4 protocol  match ipv4 source address  match ipv4 destination address  match transport source-port  match transport destination-port  match interface input  match flow direction  collect routing next-hop address ipv4  collect counter bytes |
| Konfiguration des Netflow Monitors | flow monitor <flow monitor name>  export <flow exporter name>  record <flow record name>  cache timeout inactive 60  cache timeout active 60  cache timeout update 1 |
| Binden von Netflow an das Interface | interface GigabitEthernet<ID>/<ID>  ip flow monitor <flow monitor name> input |

Tabelle 15: IOS-basierte System – Netflow

## VLAN Trunking Protocol (VTP)

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Deaktivieren von VTP | vtp version 2  vtp domain <domain-name>  vtp mode transparent |

Tabelle 16: IOS-basierte System – VLAN Trunking Protocol (VTP)

## Nicht genutzte Ports aus dem Default-VLAN entfernen

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| verschieben der nicht genutzten Ports aus dem Default-VLAN | VLAN<VLAN-ID-Unused-Ports>  name Unused-Ports  !  interface range gigabitethernet <slot>/<start-interface> - <end-interface>  switchport access vlan <VLAN-ID-Unused-Ports>  switchport mode access  shutdown |

Tabelle 17: IOS-basierte System – verschieben der nicht genutzten Ports

## Aktivieren von Port-Security zum Schutze vor MAC-Flooding

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Konfigurieren der Port-Security zum Schutze vor Mac-Flooding  Es sind 5 Mac-Adressen erlaubt. Sollte eine weitere hinzukommen wird ein SNMP-Trap ausgelöst | interface range gigabitethernet <slot>/<start-interface> - <end-interface>  switchport mode access  switchport port-security  switchport port-security maximum 5  switchport port-security violation restrict |

Tabelle 18: IOS-basierte Systeme – Aktivieren von Port-Security zum Schutze vor MAC-Flooding

## Traffic Storm Control

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Setzen der Traffic Storm Control Werte | interface range gigabitethernet <slot>/<start-interface> - <end-interface>  storm-control broadcast level bps 10m  storm-control multicast level bps 10m  storm-control action trap |

Tabelle 19: IOS-basierte Systeme – Traffic Storm Control

## Konfiguration des EtherChannel

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Verknüpfen der physikalischen Interface mit dem EtherChannel  Deaktivieren von LAcP und PAgP | interface gigabitethernet <slot>/<last-interface>  channel-group <ID> mode on |
| Abschließende Konfiguration des EtherChannel | interface port-channel <ID>  switchport mode trunk encapsulation dot1q  switchport mode trunk |
| Deaktivieren von Dynamic Trunk Protokollen | switchport nonegotiate |
| im Interface-Konfigurationsmodus wird das native VLAN gesetzt | switchport trunk native vlan <nativ-vlan-id> |
| im Interface-Konfigurationsmodus werden die dediziert erlaubten VLANs pro Trunk konfiguriert | switchport trunk allow vlan <vlan-id> |
| Optimierung des Load-Balancing Verhaltens im globalen Konfigurationsmodus für die WAN-Verbindung | port-channel load-balance src-dst-ip |

Tabelle 20: IOS-basierte System – Konfiguration EtherChannel

## Konfiguration des Trunk-Ports

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Das Interface mit der höchsten ID wird zum Trunk-Port konfiguriert | interface gigabitethernet <slot>/<last-interface>  description +++ <slot>/<last-interface> connected to <destination> +++ |
| Der bisherige Access-Port wird zum Trunk-Port im Interface-Konfigurationsmodus um konfiguriert | switchport mode trunk encapsulation dot1q  switchport mode trunk |
| Deaktivieren von Dynamic Trunk Protokollen | switchport nonegotiate |
| im Interface-Konfigurationsmodus wird das native VLAN gesetzt | switchport trunk native vlan <nativ-vlan-id> |
| im Interface-Konfigurationsmodus werden die dediziert erlaubten VLANs pro Trunk konfiguriert | switchport trunk allow vlan <vlan-id> |

Tabelle 21: IOS-basierte System – Konfiguration des Trunk-Ports

# Empfehlungen für NX-OS-basierte Systeme

## NTP

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegung der NTP Parameter und des max. 8-stelligen Hashes zur Authentisierung | ntp authenticate  ntp authentication-key <key-id> md5 <hash>  ntp trusted-key <key-id>  ntp maxdistance 1  ntp broadcastdelay 0  ntp peer <peer\_address> key <key-id>  ntp server <server\_address> key <key-id> |

Tabelle 22: NX-OS-basierte System - NTP Vorgaben

## Zeitzone und automatische Umschaltung

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| MET ist die Zeitzone und automatisches Umschalten zwischen Winter und Sommerzeit soll aktiviert werden | clock timezone CET 1 0  clock summer-time CEST 1 Sunday March 2:00 1 Sunday October 3:00 60 |

Tabelle 23: NX-OS-basierte System - Zeitzone und automatische Umschaltung

## Lokale Benutzer und TACACS+

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Aktivieren des Passwort-Secure-Modus | password secure-mode |
| Lokale Nutzer für Notfallzugriff | username <notfallbenutzer> secret <Passwort> expire <YYYY-MM-DD> role <network-admin|network-operator|vdc-admin|vdc-operator|priv-15| priv-14| priv-13| priv-12| priv-11| priv-10| priv-9| priv-8| priv-8| priv-7| priv-6| priv-5| priv-4| priv-3| priv-2| priv-1| priv-0> |
| Anzahl der erlaubten fehlerhaften Anmeldeversuche | aaa authentication rejected 5 in 180 ban 3600 |
| Festlegen der IP-Adressen des TACACS-Servers für die Authentisierung. | tacacs-server host <1. TACACS-IP-Add> key <Passwort>  tacacs-server host <2. TACACS-IP-Add> key <Passwort>  aaa group server tacacs+ <TACACS-GROUP>  server <1. TACACS-IP-Add>  server <2. TACACS-IP-Add>  use-vrf management  deadtime 15 |
| AAA Konfiguration | aaa authentication login default group <TACACS-GROUP>  aaa authentication login default fallback error local  !  aaa authentication login console group <TACACS-GROUP>  aaa authentication login console fallback error local  !  aaa authentication login invalid-username-log |

Tabelle 24: NX-OS-basierte System – lokale Benutzer und TACACS+

## Telnet-Server

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Deaktivieren des Telnet Services/Servers | no feature telnet |

Tabelle 25: NX-OS-basierte System – Telnet-Server

## SSH-Server

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegen der SSH-Server version sowie Umsetzung von Härtungsmaßnahmen | no feature ssh  ssh key rsa 2048 force  feature ssh  ssh login-gracetime 60  ssh login-attemps 3  feature sftp-server  feature scp-server |

Tabelle 26: NX-OS-basierte System – SSH-Server

## Terminal (VTY)-Filterliste

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Erstellen der VTY-Filterliste | ip access-list <VTY-ACL-Name>  permit ip <IP-Netz> <Netz-Maske>  statistics per-entry  deny ip any any log |

Tabelle 27: NX-OS-basierte System – VTY-Filterliste

## Terminal (VTY) Console-Ports

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Terminal (VTY) - | line vty  session-limit 15  absolute-timeout 20  logout-warning 60  access-class <VTY-ACL-Name> |
| Telnet nicht erlauben | no feature telnet |

Tabelle 28: NX-OS-basierte System – VTY und Console

## Monitoring und Reporting (only snmp)

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| SNMP globale Authentisierung aktivieren | snmp-server globalEnforcePriv |
| Filter-Liste zum Eingrenzen der erlaubten IP-Adressen für den lesenden Zugriff | ip access-list <snmp-RO>  remark Dienstleister  permit ip <IP-Netz> <Netz-Maske> |
| Filter-Liste zum Eingrenzen der erlaubten IP-Adressen für den schreibenden Zugriff | ip access-list <snmp-RW>  remark NMC  permit ip <IP-Netz> <Netz-Maske>  remark Mng-Tool  permit ip <IP-Netz> <Netz-Maske> |
| SNMP-Parameter für den lesenden Zugriff festlegen. | snmp-server user <read-user> <network-admin|network-operator|vdc-admin|vdc-operator> auth sha <PASSWORD> priv aes-128 <PRIV-PASSWORD  snmp-server user <read-user> use-ipv4acl <snmp-RO> |
| SNMP-Parameter für den schreibenden Zugriff festlegen. | snmp-server user <write-group> <network-admin|network-operator|vdc-admin|vdc-operator> auth sha <PASSWORD> priv aes-128 <PRIV-PASSWORD  snmp-server user <write-user> use-ipv4acl <snmp-RW> |

Tabelle 29: NX-OS-basierte System – Monitoring und Reporting

## Spanning-Tree anpassen

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Festlegen des STP-Modus (dies ist der default) | spanning-tree mode rapid-pvst |
| alle Access-Ports von der SPT-Root-Elektion ausschließen | interface gigabitethernet <slot>/<interface>  spanning-tree port type edge  spanning-tree bpduguard enable |
| Alle Access-Ports die ein BPDU-Paket empfangen sollen abgeschaltet werden | interface gigabitethernet <slot>/<interface>  spanning-tree bpduguard enable |

Tabelle 30: IOS-basierte System – Spanning-Tree anpassen

## NetFlow

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Aktivieren der Funktion | Feature netflow |
| Konfiguration des Netflow Exporter | flow exporter <flow exporter name>  destination <IP-address from flow-collector> |
| Konfiguration des Netflow Records | flow record <flow record name>  match ip tos  match ip protocol  match ipv4 protocol  match ipv4 source address  match ipv4 destination address  match transport source-port  match transport destination-port  collect routing next-hop address ipv4  collect counter bytes |
| Konfiguration des Netflow Monitors | flow monitor <flow monitor name>  export <flow exporter name>  record <flow record name> |
| Binden von Netflow an das Interface | interface GigabitEthernet<ID>/<ID>  ip flow monitor <flow monitor name> inputo |

Tabelle 31: NX-OS-basierte System – Netflow

## VLAN Trunking Protocol (VTP)

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Deaktivieren von VTP | no feature vtp |

Tabelle 32: NX-OS-basierte System – VLAN Trunking Protocol (VTP)

## Nicht genutzte Ports aus dem Default-VLAN entfernen

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| verschieben der nicht genutzten Ports aus dem Default-VLAN | VLAN<VLAN-ID-Unused-Ports>  name Unused-Ports  !  interface gigabitethernet <slot>/interface>  switchport access vlan <VLAN-ID-Unused-Ports>  switchport mode access  shutdown |

Tabelle 33: NX-OS-basierte System – verschieben der nicht genutzten Ports

## Aktivieren von Port-Security zum Schutze vor MAC-Flooding

| **Beschreibung** | **Befehl - Feldname** |
| --- | --- |
| Konfigurieren der Port-Security zum Schutze vor Mac-Flooding  Es sind 5 Mac-Adressen erlaubt. Sollte eine weitere hinzukommen wird ein SNMP-Trap ausgelöst | interface gigabitethernet <slot>/interface>  switchport mode access  switchport port-security  switchport port-security maximum 5  switchport port-security violation restrict |

Tabelle 34: NX-OS-basierte System – Aktivieren von Port-Security zum Schutze vor MAC-Flooding