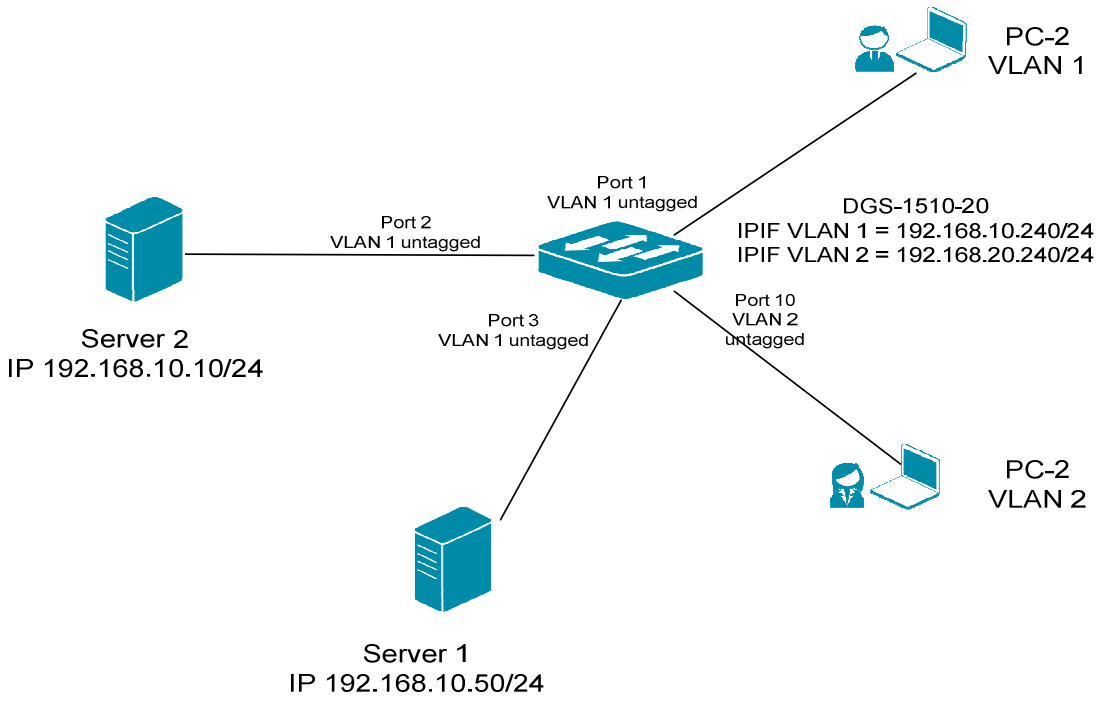
HowTo: Access Control List (ACL)

[Voraussetzungen]

1. DGS-1510-xx mit aktueller Firmware 1.10.05 und höher
2. Vorbereitete VLAN Konfiguration (z.B. lt. Anleitung ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation/DGS-1510_Series_Konfigurationsempfehlung_VLAN.pdf)
3. Vorbereitetes Routing (z.B. lt. Anleitung ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation/DGS-1510_Series_HowTo_Routing.pdf)

[Topologie]



[Vorbereitung]

- ⇨ Der DGS-1510-xx hat im Auslieferungszustand die Standard IP 10.90.90.90/8
- ⇨ Bitte ändern Sie dies bei der Ersteinrichtung (Integration in Ihre bestehende Infrastruktur) des DGS-1510-xx in Ihrem Netzwerk, für die genaue Vorgehensweise der Einstellung der IP & des Benutzernamens schlagen Sie bitte im Handbuch (z.B.: ftp://ftp.dlink.de/dgs/dgs-1510-20/documentation) nach
- ⇨ stellen Sie zudem sicher, dass die Layer 2 VLAN Konfiguration bereits erfolgt ist
- ⇨ die ACL arbeitet nur für Pakete, welche an den Ports ankommen, abgehende Pakete werden nicht gefiltert

[Aufgabe 1]

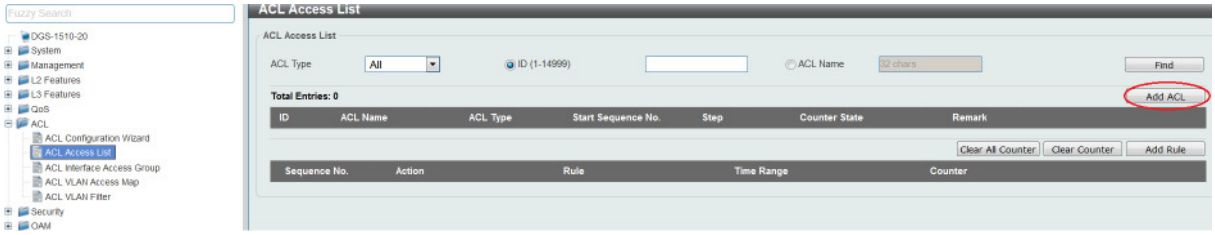
Es soll aus VLAN 2 nur auf den Server 1 (192.168.10.10/24) zugegriffen werden können, jegliche weitere Kommunikation aus VLAN 2 soll unterbunden werden.

[ACL (Access Control List) anlegen]

1.) **Verbinden zum Switch (z.B. 192.168.10.240)**

a. **ACL -> ACL Access List**

b. **Mittels „Add ACL“ legen Sie eine neue ACL an**



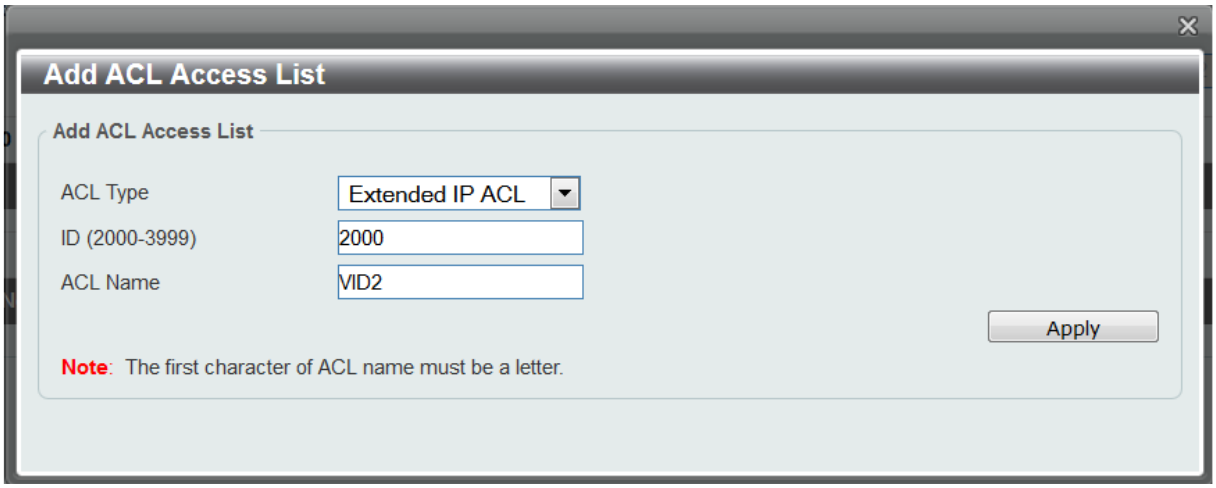
c. **wählen Sie nun ein was für eine ACL sie anlegen möchten (in diesem Beispiel eine „Extended IP ACL“)**

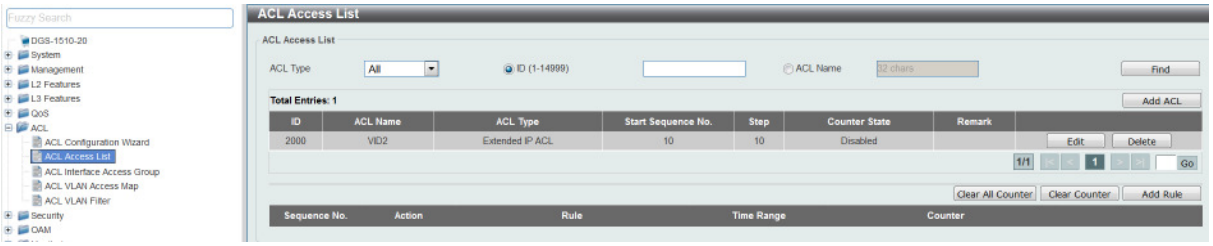
i. **ACL Type „Extendes IP ACL“**

ii. **ID Nummer 2000-3999 (z.B. 2000)**

iii. **ACL Bezeichnung (z.B. VID2)**

iv. **Mittels „Apply“ bestätigen Sie das Anlegen der ACL**

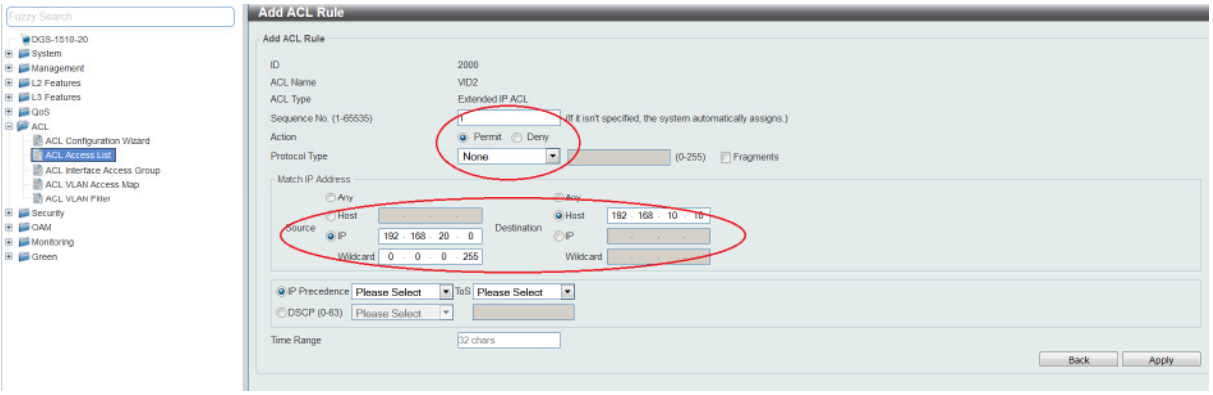


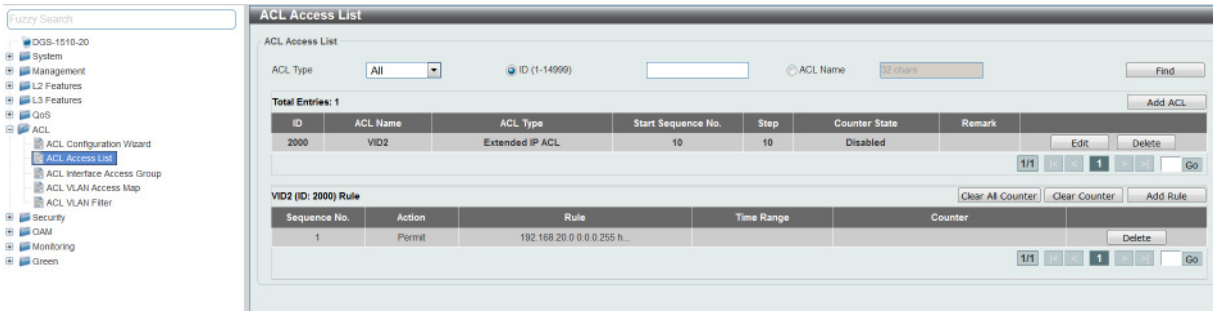


Fügen Sie erst eine entsprechende PERMIT-Regel zur ACL hinzu, so dass der dedizierte Datenverkehr aus VLAN 2 in das VLAN 1 zugelassen wird.

1. **Wählen Sie nun die ACL ID 2000 aus, indem Sie darauf clicken**
    a. **danach können Sie mittels „Add Rule“ eine neue Regel zur ACL hinzufügen**

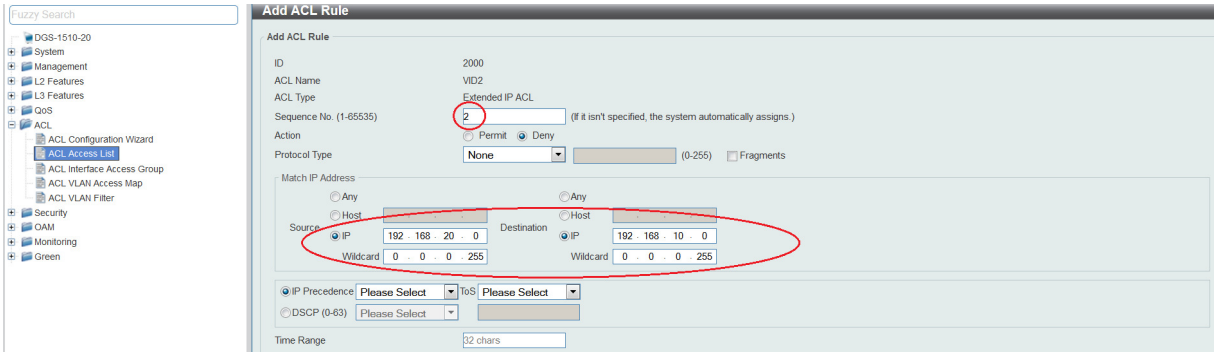
    b. **definieren Sie die Sequenz-Nummer (Reihenfolge der einzelnen Regeln „First Match“!)**
    c. **definieren Sie ob dies eine „Permit“ oder „Deny“ Regel ist**
    d. **definieren Sie das zu Regelnde Protokoll, bei Auswahl von „None“ wird ALLES geregelt**
    e. **definieren Sie die Quelle (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)**
    f. **definieren Sie das Ziel (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)**
    g. **mittels „Apply“ bestätigen Sie Ihre Eingabe**

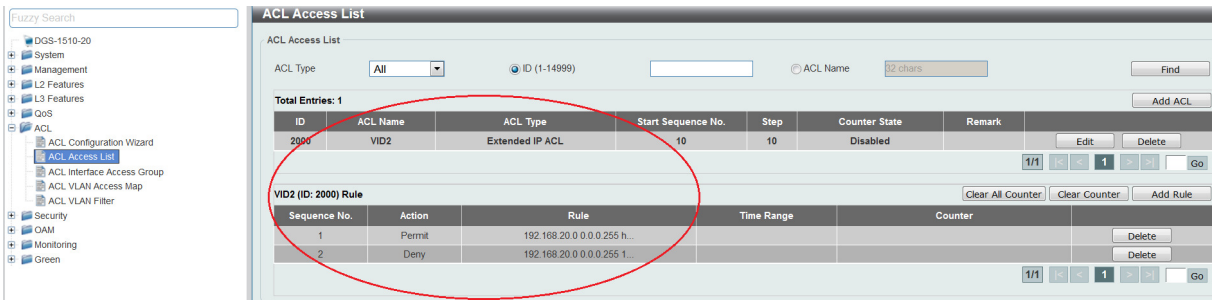




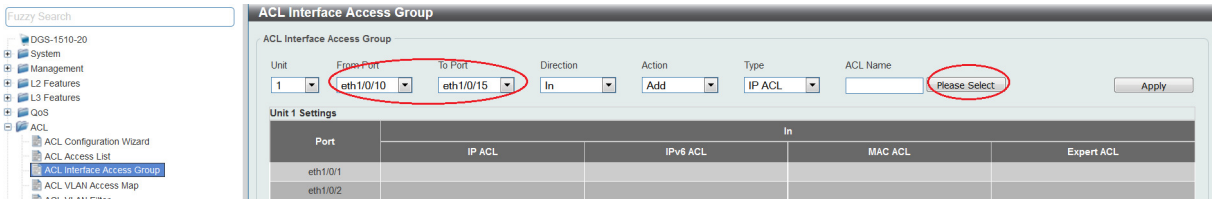
Fügen Sie nun eine entsprechende DROP-Regel zur ACL hinzu, so dass der Datenverkehr aus VLAN 2 in das VLAN 1 blockiert wird.

1. **Wählen Sie nun erneut die ACL ID 2000 aus, indem Sie darauf clicken**
   - h. **danach können Sie mittels „Add Rule“ eine neue Regel zur ACL hinzufügen**
   - i. **definieren Sie die Sequenz-Nummer (Reihenfolge der einzelnen Regeln „First Match“!)**
   - j. **definieren Sie ob dies eine „Permit“ oder „Deny“ Regel ist**
   - k. **definieren Sie das zu Regelnde Protokoll, bei Auswahl von „None“ wird ALLES geregelt**
   - l. **definieren Sie die Quelle (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)**
   - m. **definieren Sie das Ziel (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)**
   - n. **mittels „Apply“ bestätigen Sie Ihre Eingabe**

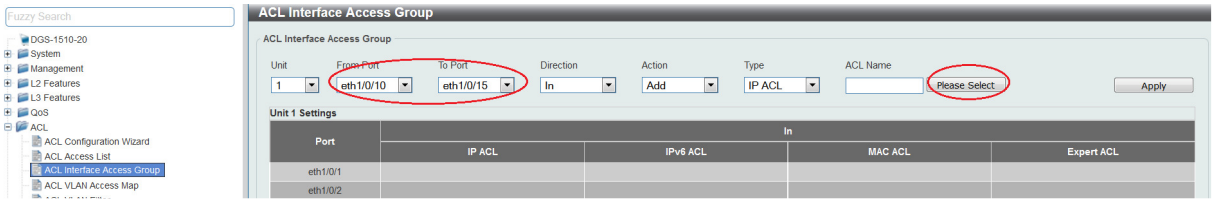


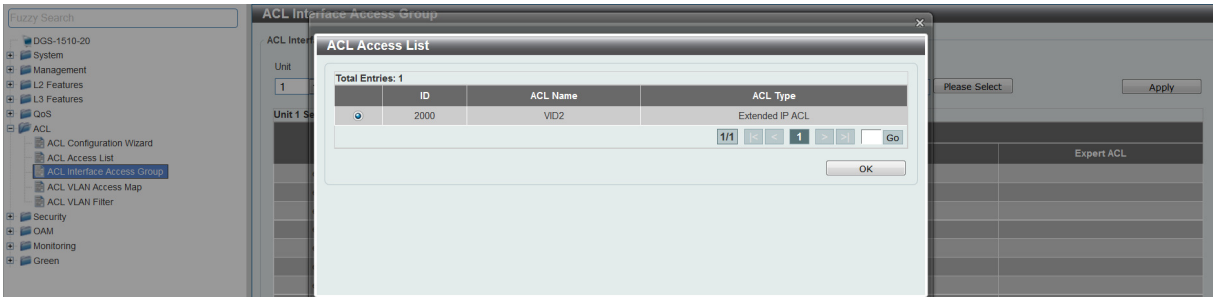


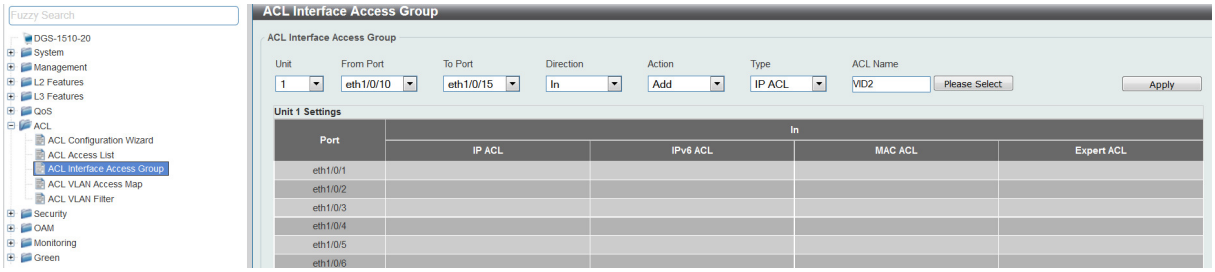
Sie haben somit eine ACL mit 2 Regeln erstellt.
Die Regel 1 erlaubt den Zugriff aus VLAN 2 auf den Server IP 192.168.10.10.
Die Regel 2 blockiert allen Zugriff aus VLAN 2 auf das VLAN 1.

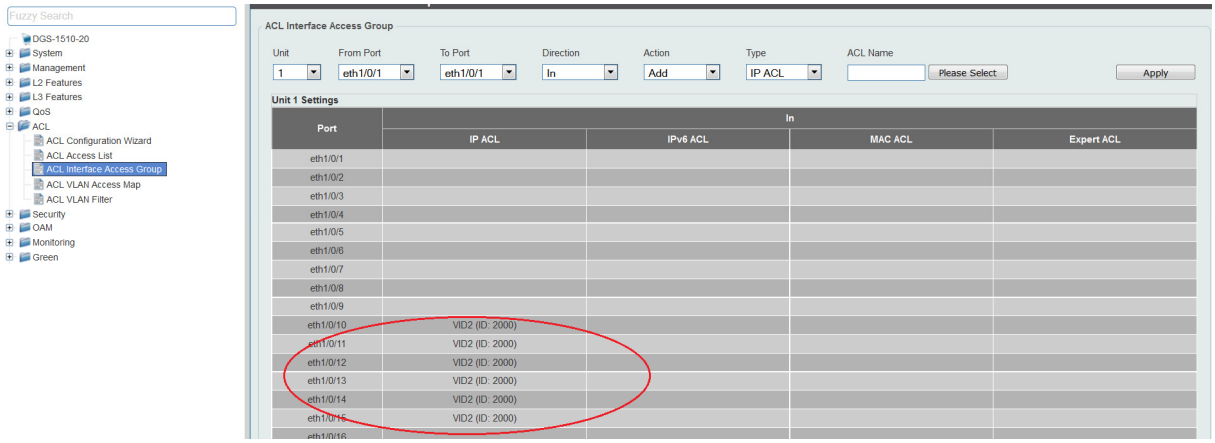


a. **Fügen Sie nun die entsprechende ACL einem/mehreren Ports hinzu**
   a. **ACL -> ACL Interface Access Group**
   b. **Wählen Sie die „ingress Ports“ aus**
   c. **Mittels „Add/Delete“ können Sie die ACL einem Port hinzufügen oder löschen**
   d. **Bei „Type“ wählen Sie Ihren erstellten ACL Typ aus**
   e. **Bei „Please Select“ werden Ihnen alle erstellten ACLs angezeigt**
   f. **Wählen Sie nun Ihre entsprechende ACL aus**
   g. **Mittels „Apply“ binden Sie nun die ACL auf die entsprechenden Ports**



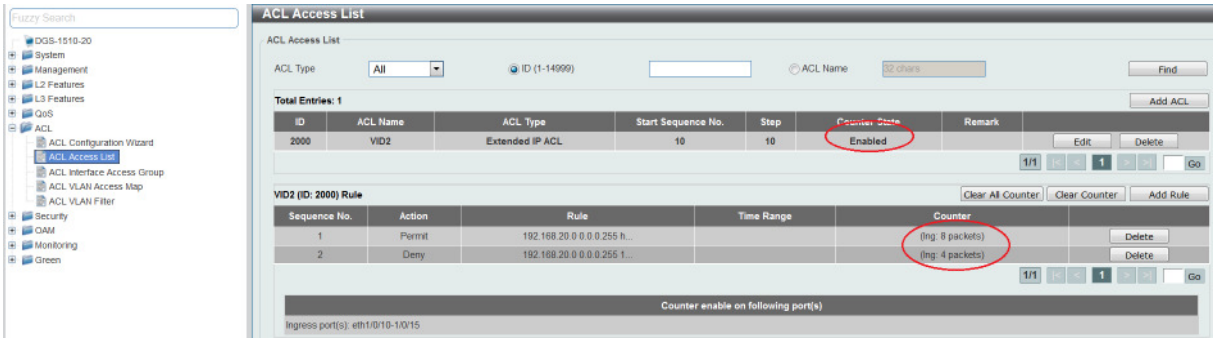






Sobald Sie die ACL auf den Port gebunden haben, wird der entsprechende Datenverkehr gemäß der ACL zugelassen oder blockiert.

Sollten Sie die Counter aktiviert haben, so können Sie unter ACL Access List den Hit-Count einsehen.



Stellen Sie bei der Erstellung von ACLs sicher, dass Ihr Administrations-PC nicht durch eine entsprechende ACL/Regel blockiert wird!

Bitte beachten Sie, dass Sie alle Anpassungen entsprechend speichern. Ein APPLY ist kein permanentes Speichern!