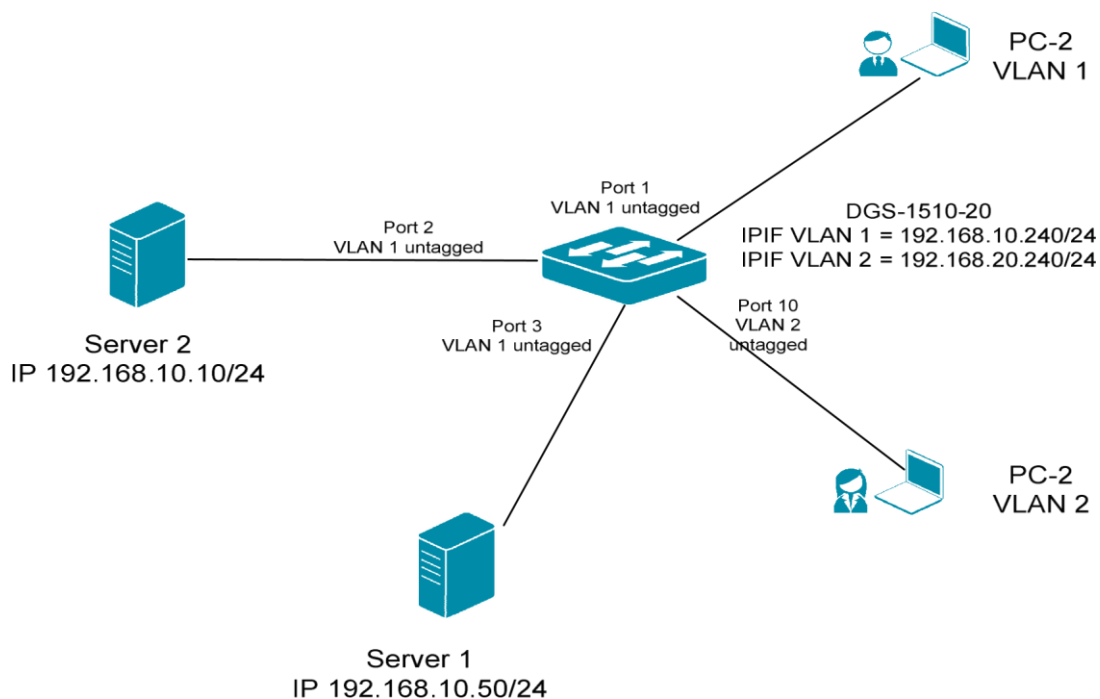


HowTo: Access Control List (ACL)

[Voraussetzungen]

1. DGS-1510-xx mit aktueller Firmware 1.7.0 und höher
2. Vorbereitete VLAN Konfiguration (z.B. lt. Anleitung https://ftp.dlink.de/dgs/dgs-1510/documentation/HowTo/dgs-1510_howto_Konfigurationsempfehlung_VLAN.pdf)
3. Vorbereitetes Routing (z.B. lt. Anleitung https://ftp.dlink.de/dgs/dgs-1510/documentation/HowTo/dgs-1510_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.: <https://ftp.dlink.de/dgs/dgs-1510/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

[Beispiel 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.

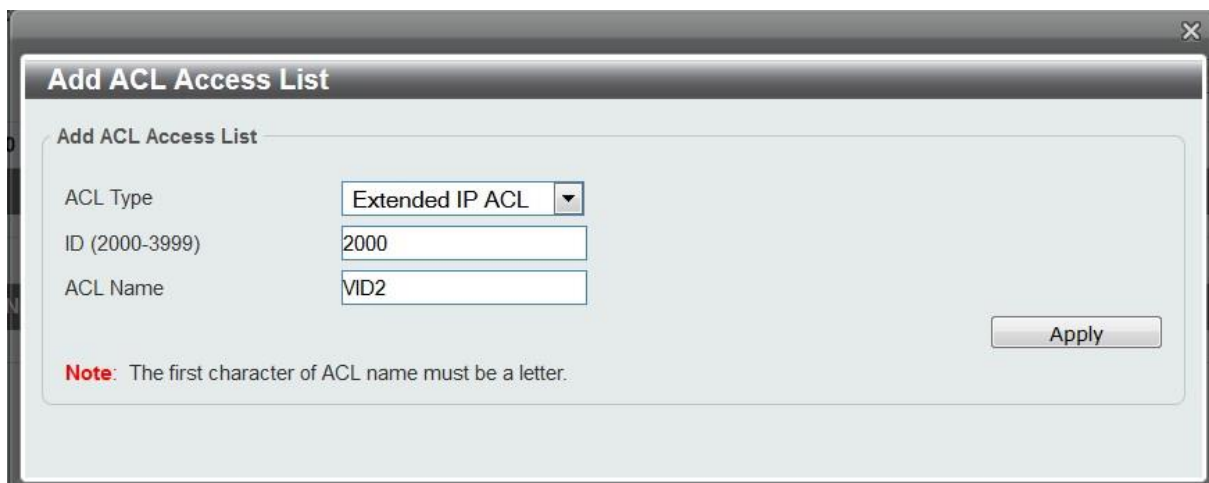
[ACL (Access Control List) anlegen]

1. Verbinden zum Switch (z.B. 192.168.10.240)
2. ACL -> ACL Access List
3. Mittels „Add ACL“ legen Sie eine neue ACL an





4. Wählen Sie nun ein was für eine ACL sie anlegen möchten (in diesem Beispiel eine „Extended IP ACL“)
5. ACL Type „Extended IP ACL“
6. ID Nummer 2000-3999 (z.B. 2000)
7. ACL Bezeichnung (z.B. VID2)
8. Mittels „Apply“ bestätigen Sie das Anlegen der ACL

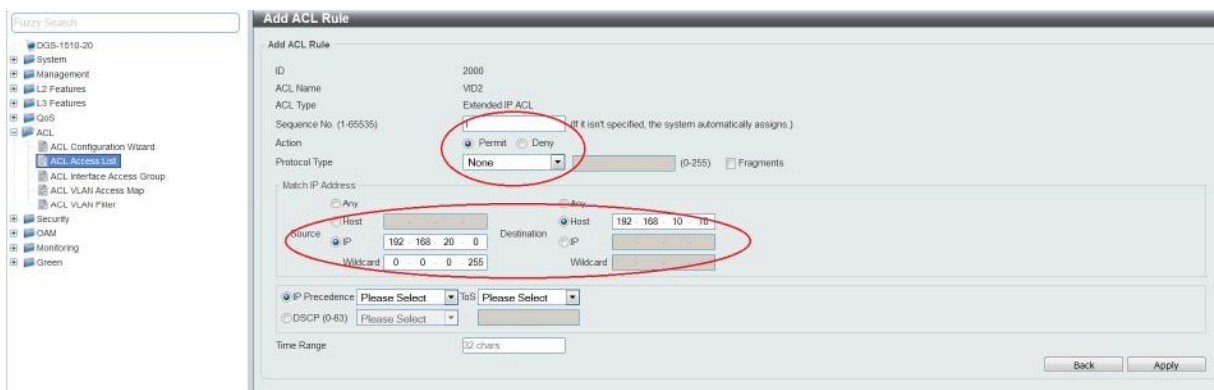


Fügen Sie erst eine entsprechende PERMIT-Regel zur ACL hinzu, so dass der dedizierte Datenverkehr aus VLAN 2 in das VLAN 1 zugelassen wird.

1. Wählen Sie nun die ACL ID 2000 aus, indem Sie daraufklicken
2. Danach können Sie mittels „Add Rule“ eine neue Regel zur ACL hinzufügen



3. Definieren Sie die Sequenz-Nummer (Reihenfolge der einzelnen Regeln „First Match“!)
4. Definieren Sie ob dies eine „Permit“ oder „Deny“ Regel ist
5. Definieren Sie das zu Regelnde Protokoll, bei Auswahl von „None“ wird ALLES geregelt
6. Definieren Sie die Quelle (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)
7. Definieren Sie das Ziel (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)
8. 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.

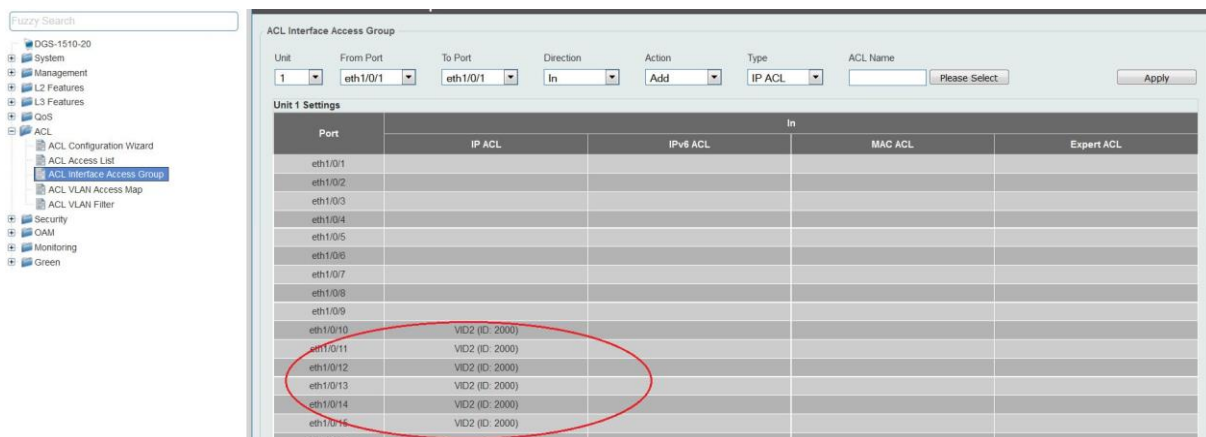
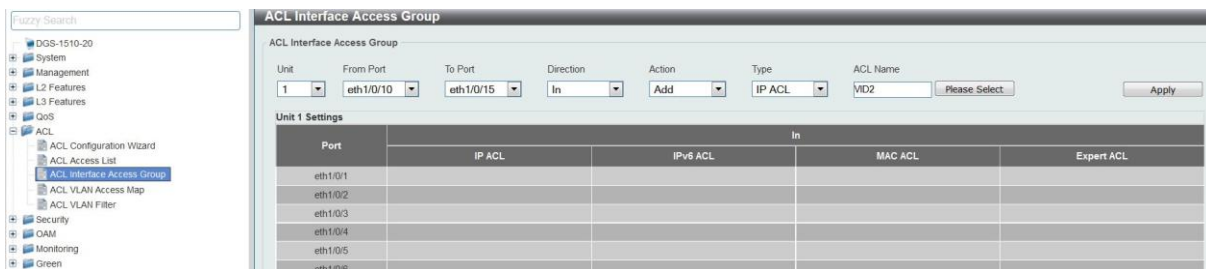
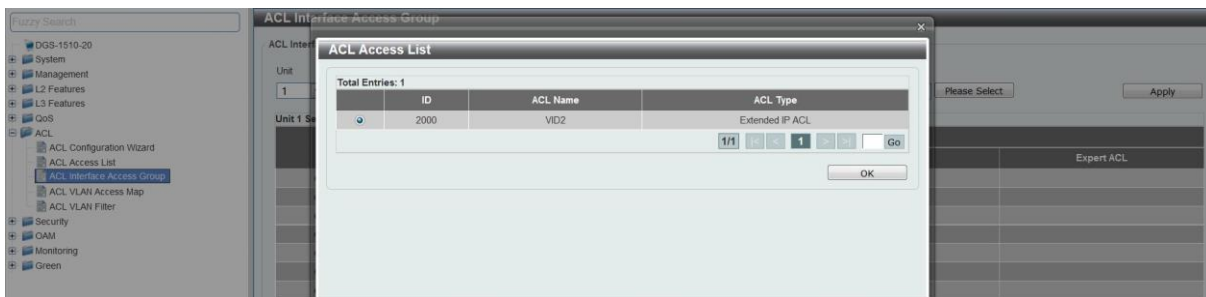
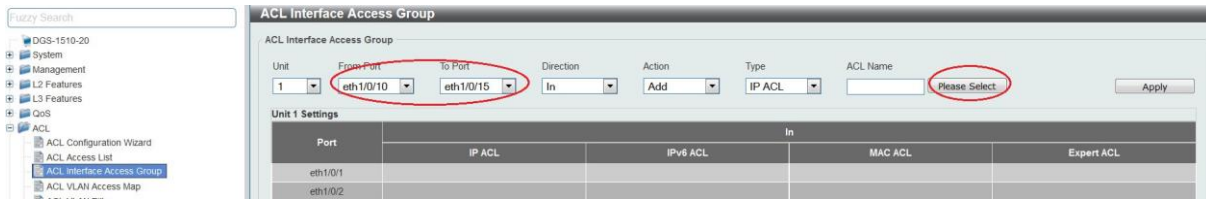
1. Wählen Sie nun erneut die ACL ID 2000 aus, indem Sie darauf klicken
2. Danach können Sie mittels „Add Rule“ eine neue Regel zur ACL hinzufügen
3. Definieren Sie die Sequenz-Nummer (Reihenfolge der einzelnen Regeln „First Match“!)
4. Definieren Sie ob dies eine „Permit“ oder „Deny“ Regel ist, definieren Sie das zugehörige Protokoll, bei Auswahl von „None“ wird ALLES geregelt
5. Definieren Sie die Quelle (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)
6. Definieren Sie das Ziel (Any = ALLES, Host = einzelner Client/IP, IP = Netzbereich mit Wildcard Subnetzmaske)
7. Mittels „Apply“ bestätigen Sie Ihre Eingabe

ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark
2000	VID2	Extended IP ACL	10	10	Disabled	

Sequence No.	Action	Rule	Time Range	Counter
1	Permit	192.168.20.0 0.0.0.255 h...		
2	Deny	192.168.20.0 0.0.0.255 1		

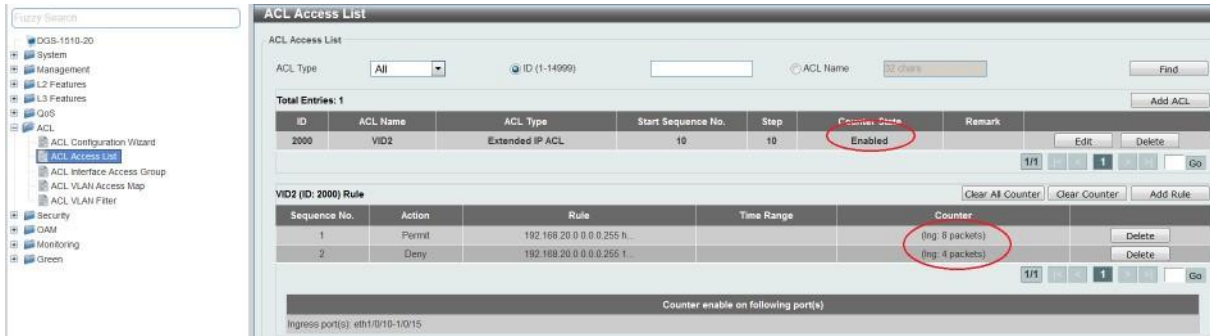
Sie haben somit eine ACL mit 2 Regeln erstellt.
 Die Regel 1 erlaubt den Zugriff aus VLAN 2 auf den Server IP 192.168.10.10.
 Die Regel 2 blockiert allen Zugriff aus VLAN 2 auf das VLAN 1.

1. Fügen Sie nun die entsprechende ACL einem/mehreren Ports hinzu
2. ACL -> ACL Interface Access Group
3. Wählen Sie die „ingress Ports“ aus
4. Mittels „Add/Delete“ können Sie die ACL einem Port hinzufügen oder löschen
5. Bei „Type“ wählen Sie Ihren erstellten ACL Typ aus
6. Bei „Please Select“ werden Ihnen alle erstellten ACLs angezeigt
7. Wählen Sie nun Ihre entsprechende ACL aus
8. 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 HitCount 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!