

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 <u>https://ftp.dlink.de/dgs/dgs-1510/documentation/HowTo/dgs-1510_howto_Konfigurationsempfehlung_VLAN.pdf</u>)
- 3. Vorbereitetes Routing (z.B. lt. Anleitung <u>https://ftp.dlink.de/dgs/dgs-1510/documentation/HowTo/dgs-1510 howto Routing.pdf</u>)

[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.: <u>https://ftp.dlink.de/dgs/dgs-1510/documentation</u>) 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





Add ACL Access List		
Add ACL Access List		
ACL Type ID (1-1999)	Standard IP ACL Standard IP ACL Extended IP ACL	
ACL Name	Standard IPv6 ACL Extended IPv6 ACL Extended MAC ACL	Apply
Note: The first character of AQ	Extended Expert ACL	

- 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

dd ACL Access List		
ACL Type	Extended IP ACL	
D (2000-3999)	2000	
ACL Name	VID2	
		Apply
Note: The first charac	ter of ACL name must be a letter.	

Fuzzy Soards	ACL Acces	s List			_				
DGS-1510-20 System Management L2 Features	ACL Access Li ACL Type	st All 💌	 D (1-14999) 		0	ACL Name			Find.
E L3 Features	Total Entries	1							Add ACL
🖲 💭 QOS	D	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark		
ACL: Configuration Wizard	2000	VED2	Extended IP ACL	10	10	Disabled	Clear All Cou	Edit Del	ete Go Add Rule
Security GAM	Sequence	No. Action	Rule		Time Range		Counter		



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

	ACL Access	List			_			
PGS-1510-20	ACL Access List							
system 💭	1000000000	10000				and and a second		1
Janagement Nanagement	ACL Type	All	ID (1-14999)	3)	04	ACL Name 12 chara	3.	Find
📁 📁 L2 Features								
📁 💭 L3 Features	Total Entries:	1						Add ACL
Dos ACI	ID	AGL Hamp	ACI Type	Start Sequence No.	Step	Counter State	Remark	
ACL Configuration Wizard	2000	VID2	Extended IP ACL	10	10	Disabled		Edit Delete
ACL Access List							1	/1 · · / G
ACL VLAN Access Map		-						11.1
ACL VLAN Filter	VID2 (ID: 2000)	Rule					Clear All Count	ter Clear Counter Add Rule
Security	Sequence I	No. Action	Rule		Time Range		Counter	
CAM .								

- 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

	Add ACL Rule
DG5-1510-20	Add ACL Rule
😟 📁 System	
🖽 📁 Management	ID 2006
E L2 Features	ACL Name VID2
🗄 💭 L3 Features	ACL Type Extended IP ACL
🐨 📕 Q0S	Experience Alle (4 02255) (19 / 10 / 10 / 10 / 10 / 10 / 10 / 10 /
🖻 🎾 ACL	oedenke we (1-0000)
ACL Configuration Wizard	Producel Type (0-255) Programments
Monitoring	Mitter 0, 0, 0, 255 Mitter
la poleen	
	@P Previdence Diagra Salact VInS Plance Salact V
	PRPP 0.031 Classes Control +
	Chook (Margh) (Marghan 201802 [1]
	Time Range 32 chars
	Back Apply
Fuzzy Sterott	ACL Access List
DGS-1510-20	ACL Access List
🛞 💭 System	
🕀 📁 Management	ACL Type All ACL Type All ACL Name States Find
🗉 📁 L2 Features	
🕀 🃁 L3 Features	Total Entries: 1 Add ACL
🖽 📁 QoS	
E PACL	ID ACLIName ACLIType Start Sequence No. Step Counter State Hemark
ACL Configuration Wizard	2000 VID2 Extended IP ACL 10 10 Disabled Edit Delete
ACL Access List	
ACL Interface Access Group	
ACL VLAN Access Map	VID2 (ID: 2000) Rule Clear Al Counter Add Rule
ACL VLAN Filter	
B Security	Sequence No. Action Rule Time Range Counter
	1 Permit 192.168.20.0.0.0.0255 h Delete
E Green	17 100



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 zu Regelnde 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

DOS-1510-20 Gostem Dos-1510-20 Gostem Management La Features Cost Act. Confournation Weard Act. Access Late Gostem Act. VuN Access Map Gostem Gostem Gostem Gostem Gostem Gostem	Add ACL Rule ID 2000 ACL Name VID2 ACL Type Estimated IP ACL Sequence No (1-65535) Permit © Derry Protocol Type None Permit © Derry (0-255) Protocol Type None Match IP Address More Widcard Destination @IP Precedence Please Select ToS Please Select Widcard Do DSCP (0-83) Please Select Time Range \$2 chars

	AGL Access Li	51			_		_	
OGS-1510-20 System Management Management L2 Features	ACL Access List	All	ID (1-14999)		_ 0	ACL Name 32 chars		Find
🗉 📁 L3 Features	Total Entries: 1							Add ACL
	ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
ACL Configuration Wizard	2000	VID2	Extended IP ACL	10	10	Disabled		Edit Delete
ACL Access List								1/1 K K 1 K Go
ACL VLAN Access Map	VID2 (ID: 2000) Ru	le					Clear All Cou	inter Clear Counter Add Rule
🖲 📁 Security	Sequence No.	Action	Rule		Time Range		Counter	
🕑 📁 OAM	1	Permit	192.168.20.0 0.0.0	.255 h				Delete
E Green	2	Deny	192.168.20.0 0.0.0	255 1				Delete
								1/1 K < 1 > > Go

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.

Fuzzy Search	ACL Interface Access G	iroup			
OGS-1510-20 System Management Iz Features IJ Features IJ Features	ACL Interface Access Group Unit From Port 1 Unit eth 1/0/10 Unit 1 Settings	To Port Direction	Action Type Add Type	ACL Name Please Sele	ct Apply
E PACL				In	
ACL Configuration Wizard	Port	IP ACL	IPv6 ACL	MAC ACL	Expert ACL
ACL Interface Access Group	eth1/0/1				
ACL VLAN Access Map	eth1/0/2				



- 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.

Fuzzy Seeron	ACL Access Lis	it						
OGS-1510-20 Josepherem Management Management	ACL Access List	Ali	🥥 ID (1-14999)		0/	ICL Name		Find
🗉 🗾 L3 Features	Total Entries: 1							Add ACL
	ID	ACL Name	ACL Type	Start Sequence No.	Step	Counter State	Remark	
ACL Configuration Vitzard ACL Access List ACL Interface Access Group	2000	VID2	Extended IP ACL	10	10	Enabled	1	Edit Delete
	1						1/1	
ACL VLAN Fitter	VID2 (ID: 2000) Rul	•					Clear All Counter	Clear Counter Add Rule
🗷 📁 Security	Sequence No.	Action	Rule		Time Range		Counter	
E GAM	1	Permit	192,168,20.0 0.0.0.	255 h		Cog	6 packets)	Delete
E Green	2	Deny	192.168.20.0 0.0.0.	266 1		Ong	4 packets)	Delete
CONTRACTORIES							1/1	
				Counter enable	on following po	τ(s)		
	Ingress port(s): e	th1/0/10-1/0/15						

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!