NetworkLife
Another packet in the network....

Cisco ACI — Contracts

VRF Behaviors - Policy Control Enforcement Preference:

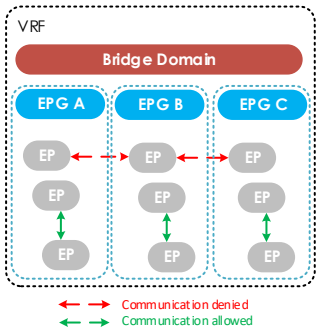
By default the VRF is « **Enforced** », the Endpoints in each EPG attached to this VRF can communicate inside an EPG, but not between EPG.

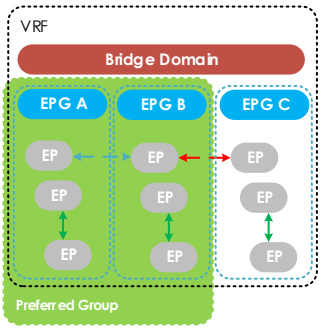
A way to configure inter-EPG communication is to enable « **Preferred-Group** » on the VRF + Enable « Preferred-Group » on each EPG.

If you set a VRF to « **Unenforced** », inter-EPG communication is allowed.

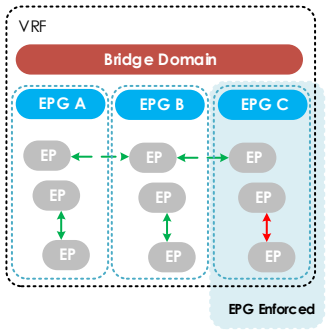
By default, **intra-EPG communication** is allowed (Unenforced), but you can Enforce an EPG to block communication between all his endpoints.

Enforced





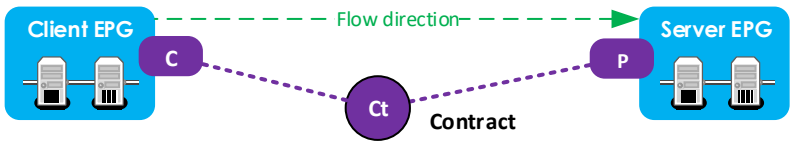
Unenforced



What is a contract inside ACI ?

Definition

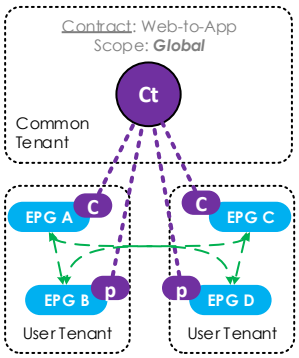
- An ACL
- Configured between EPGs, or between EPGs and L3out.
- Contracts are used to control traffic flow within the ACI fabric between EPGs.



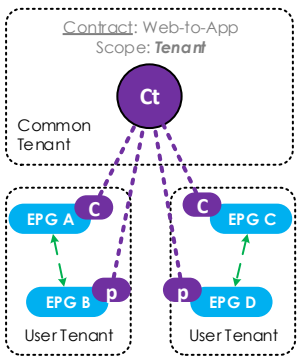
Scope

Contracts are assigned a scope of Global, Tenant, VRF, or Application Profile, which limit the accessibility of the contract.

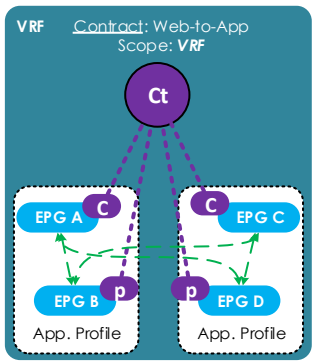
Global



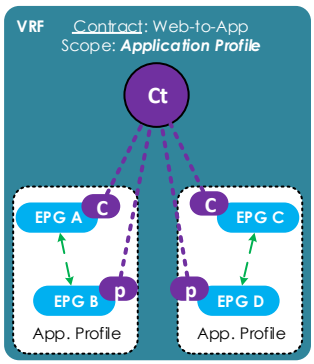
Tenant



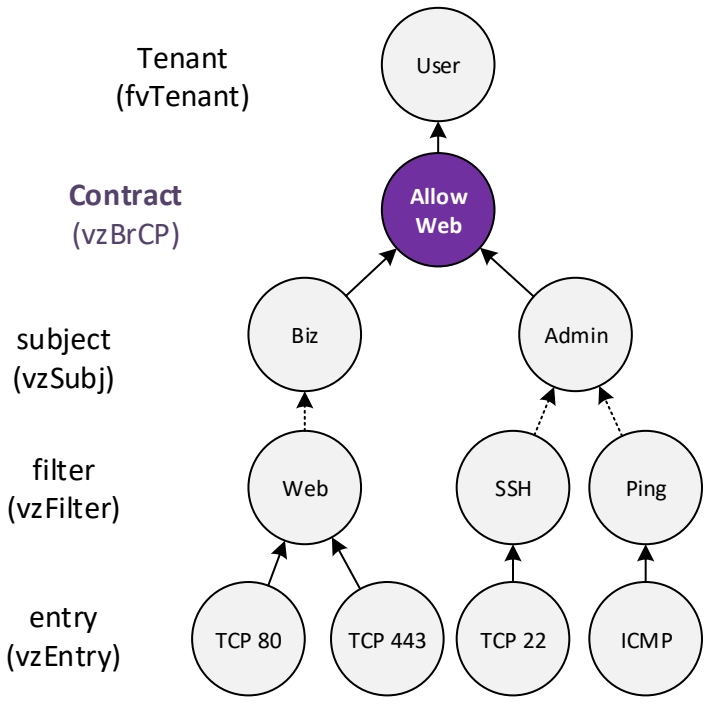
VRF



Application Profile



Object Model & Rôle



Subjects	A group of filters for a specific application or service.
Filters	Used to classify traffic based upon layer 2 to layer 4 attributes (such as Ethernet type, protocol type, TCP flags and ports)
Actions	Action to be taken on the filtered traffic.
	Permit the traffic (regular contracts, only)
	Mark the traffic (DSCP/CoS) (regular contracts, only)
	Redirect the traffic (regular contracts, only, via SG)
	Copy the traffic (regular contracts, only, via SG or SPAN)
	Block the traffic (taboo contracts, only)
	Log the traffic (taboo contracts, only)
Labels	(Optional) Used to group objects such as subjects and endpoint groups for the purpose of increasing granularity in policy enforcement.

Filters take place in the Policy CAM (on the Leaf where applied)

If you don't configure a contract, the traffic is **dropped**, except for the following specific « control-plane » traffic :

- DHCP v4 (prot 0x11, sport 0x44, dport 0x43)
- DHCP v4 (prot 0x11, sport 0x43, dport 0x44)
- DHCP v6 (prot 0x11, sport 0x222, dport 0x223)
- ND-Sol ICMPv6 (prot 0x3a dport 0x0087)
- ND-Advt ICMPv6 (prot 0x3a dport 0x0088)
- EIGRP (prot 0x58)
- IGMP (prot 0x2)
- PIM (prot 0x67)
- OSPF (prot 0x59)

Author: Benoit GONCALVES – 2020 – ACI 4.2

NetworkLife
Another packet in the network....

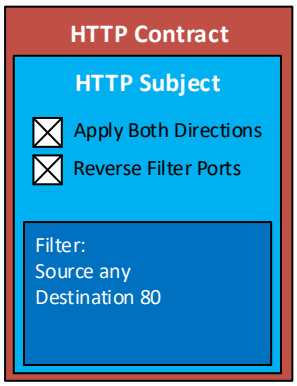
Cisco ACI — Contracts

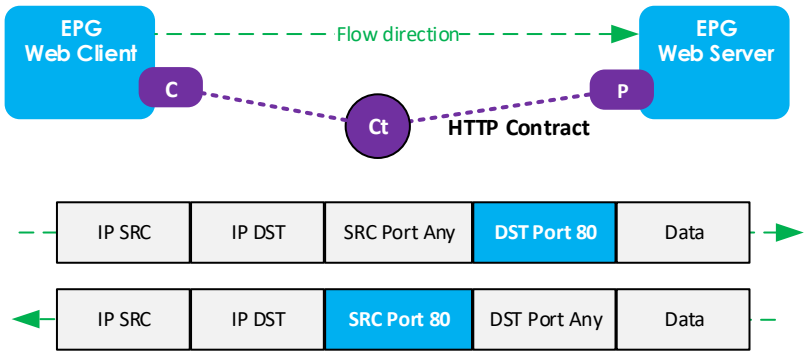
Understanding « Apply Both Direction » and « Reverse Filter Ports » options

An **HTTP Contract** is configured to match **HTTP** traffic : any source and destination port TCP 80

The **Web Client EPG consume** the HTTP Contract.
The **Web Server EPG provide** the HTTP Contract.

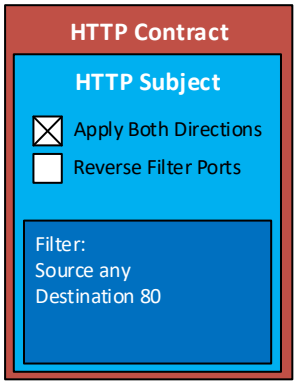
With the below configuration, the client can browse a web page: HTTP Request, and response will be allowed.

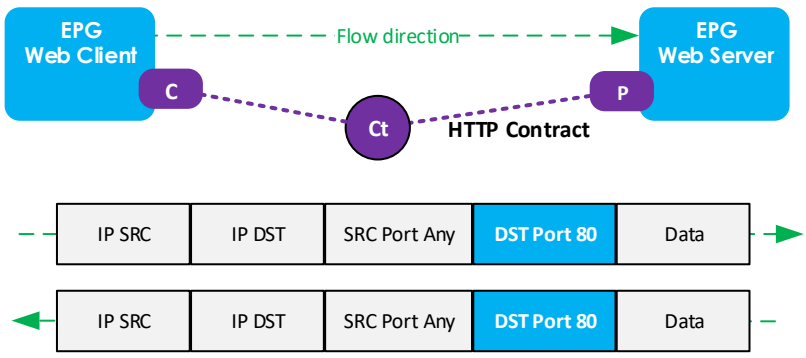




If we remove **Reverse Filter Ports** option, the contract is still applied in both directions, but with a **destination port 80** allowed in both direction.

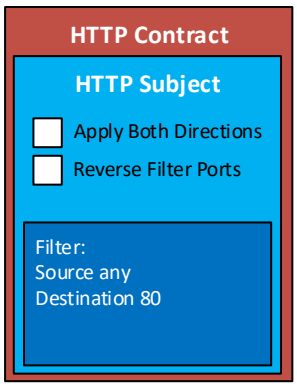
With the below configuration, the client can browse a web page: HTTP Request will be allowed, but the response is denied, unless you add a rule to allow source port TCP 80.

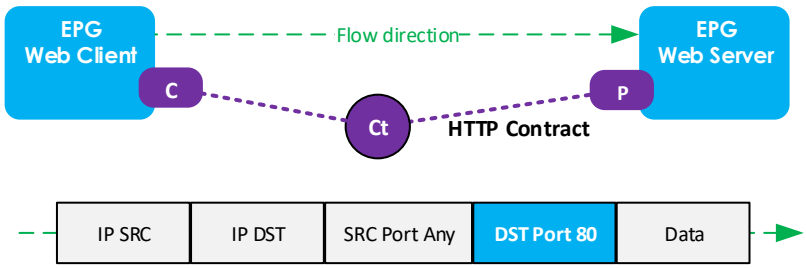




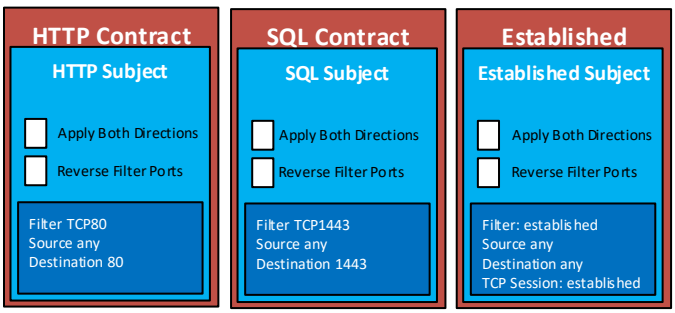
If we remove **Apply Both Directions** option, the contract is still only **applied in one direction, from consumer to provider**.

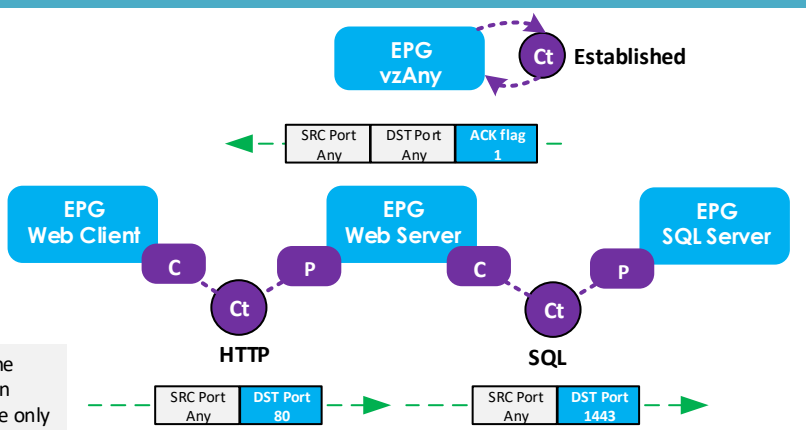
This option only **uses a single TCAM entry** rather than two as shown in the above examples.





Saving CAM table entries with **vzAny** and **TCP Established** option





The HTTP and SQL contracts allow traffic from the consuming EPGs to reach the providing EPGs, while the **Established** contract allows universal traffic between EPGs so long as the TCP session is established. The HTTP and SQL contracts are only needed to allow the initial TCP SYN packet through to establish the session. all other traffic is handled by the vzAny EPG and its Established contract.

Contracts inheritance
TCAM verification
Check contract counters & hits
Contract rule priorities
Taboo contracts

Author: Benoit GONCALVES – 2020 – ACI 4.2