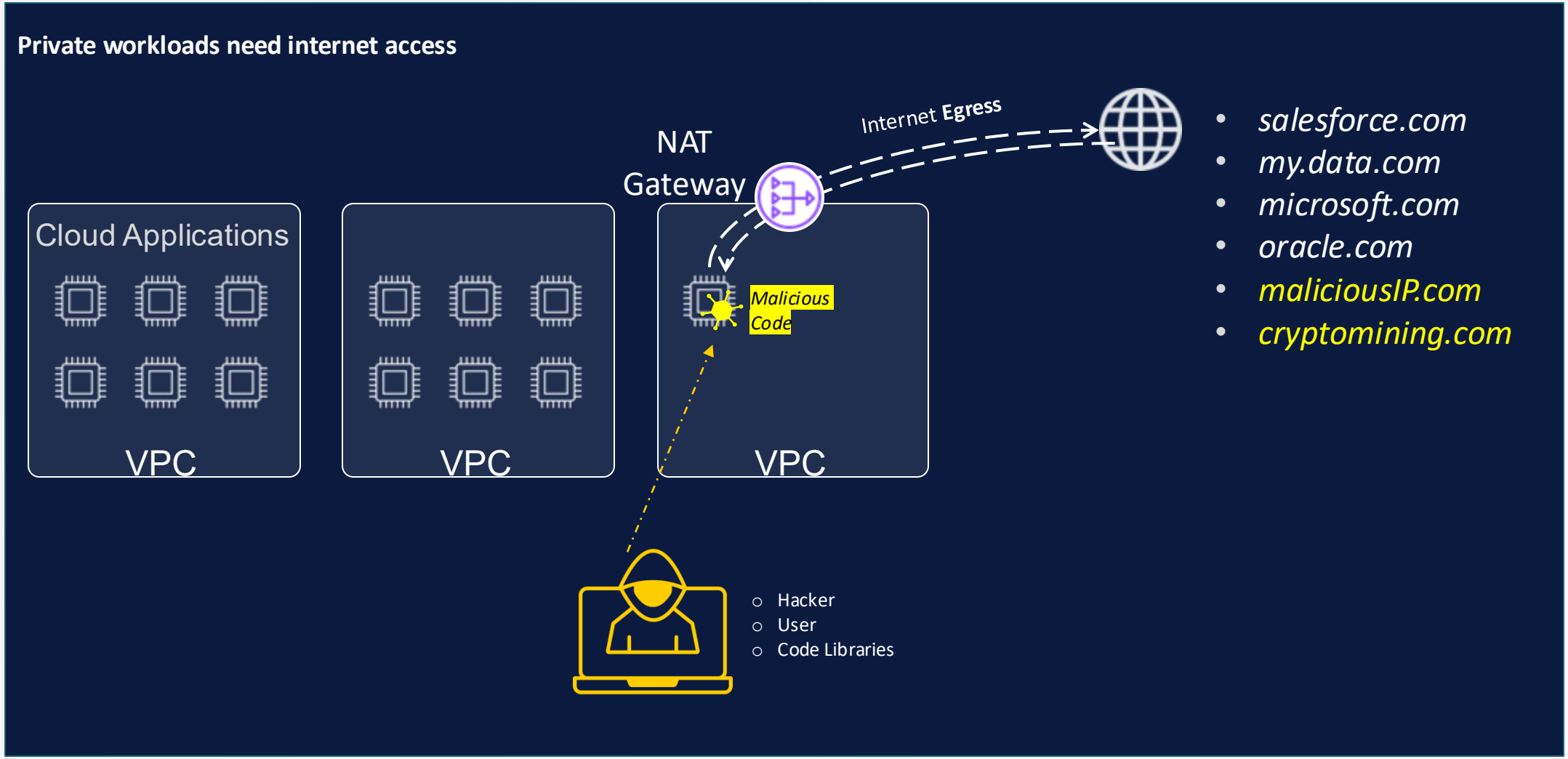
Aviatrix Cloud Firewall

Cloud Perimeter Security Basics

- SaaS integration
- Patching
- Updates

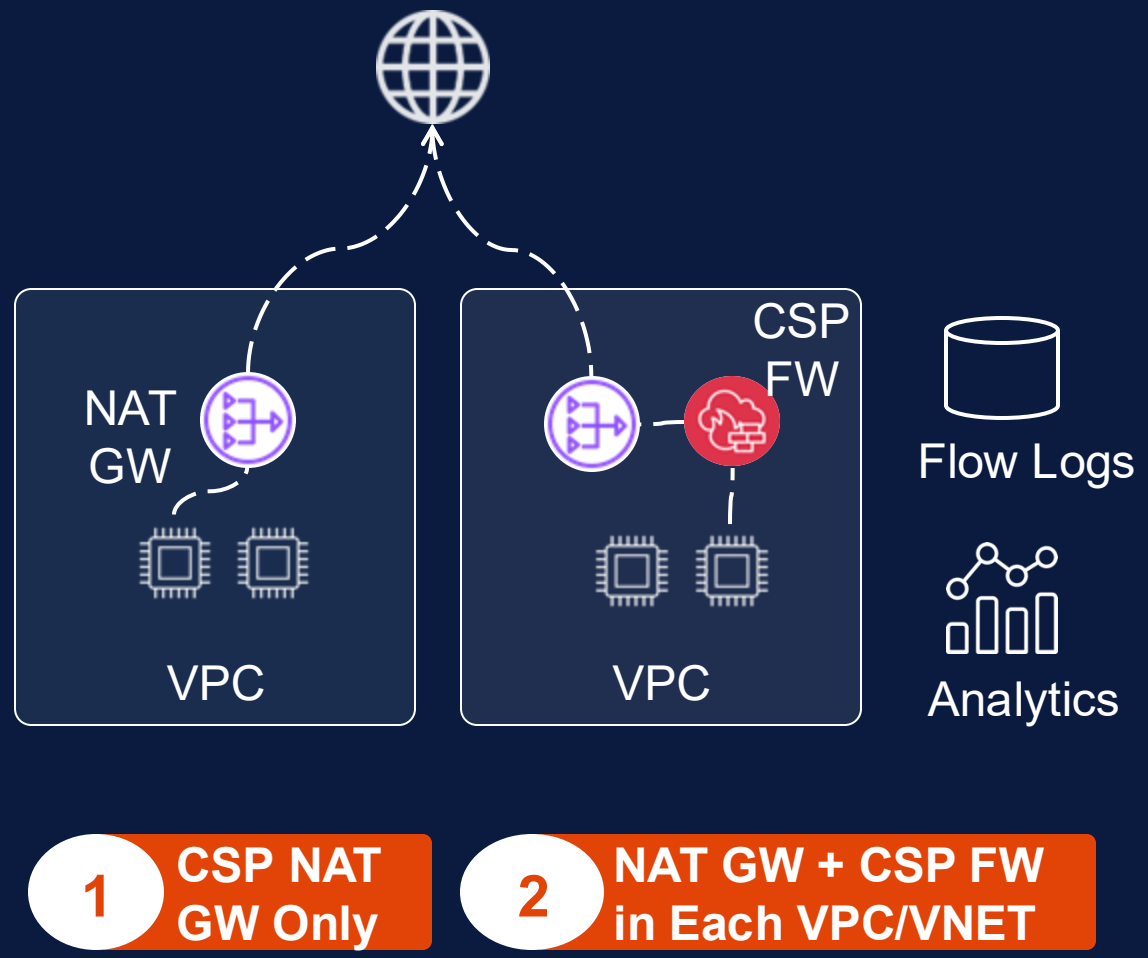


Default Architectural Options

1. CSP NAT GW Only
2. NAT GW + CSP FW in Each VPC/VNET

Challenges

- Limited visibility
- High data-processing costs
- Log storage and analytics costs
- No centralized intelligence
- Not multi-cloud capable



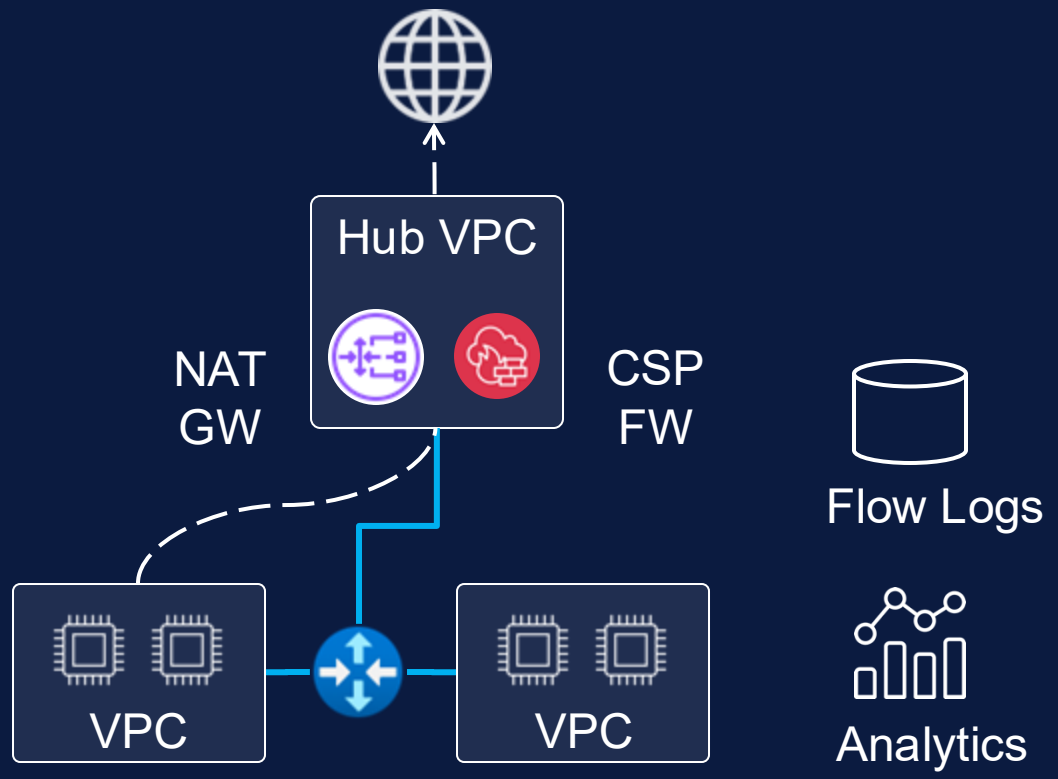
aviatrix

Default Architectural Options

3. Centralized CSP FW with Hub-and-Spoke

Challenges

- Limited visibility
- High data-processing costs
- Log storage and analytics costs
- No intelligence on new resources
- Cannot enforce encryption of data in transit
- Additional troubleshooting issues
- Not multi-cloud capable



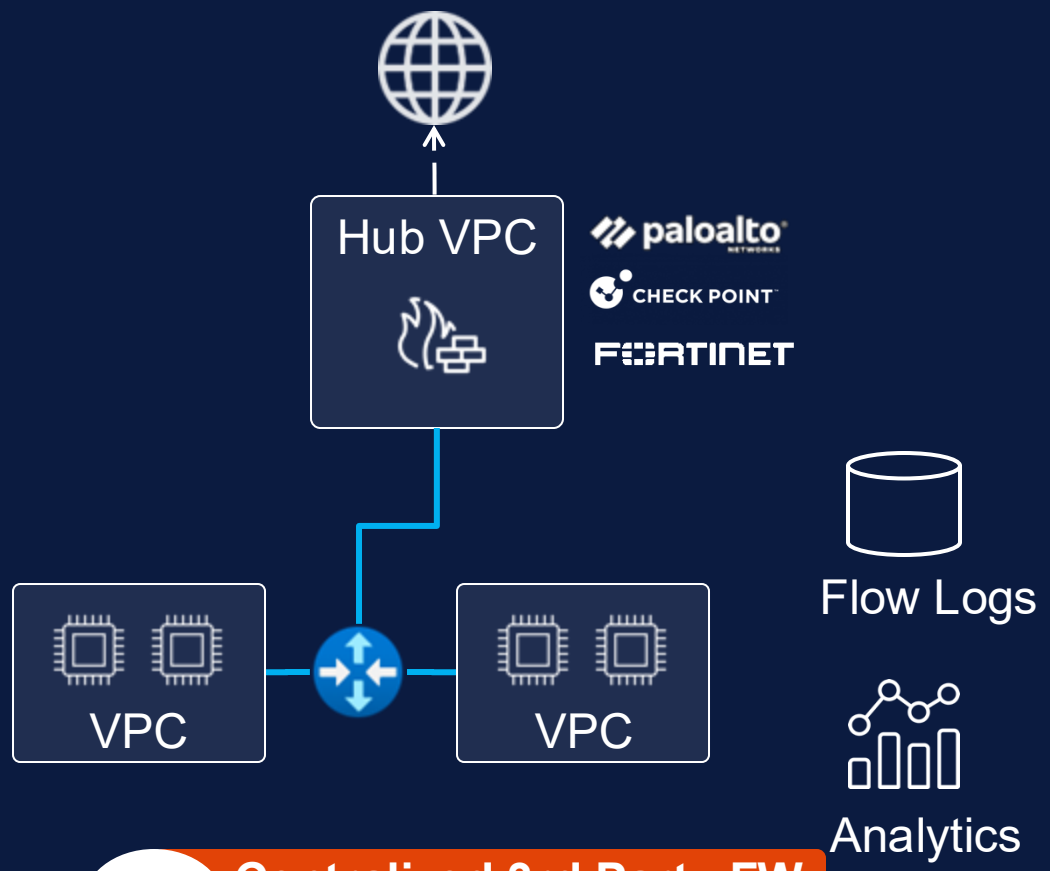
3 Centralized CSP FW with Hub-and-Spoke

Default Architectural Options

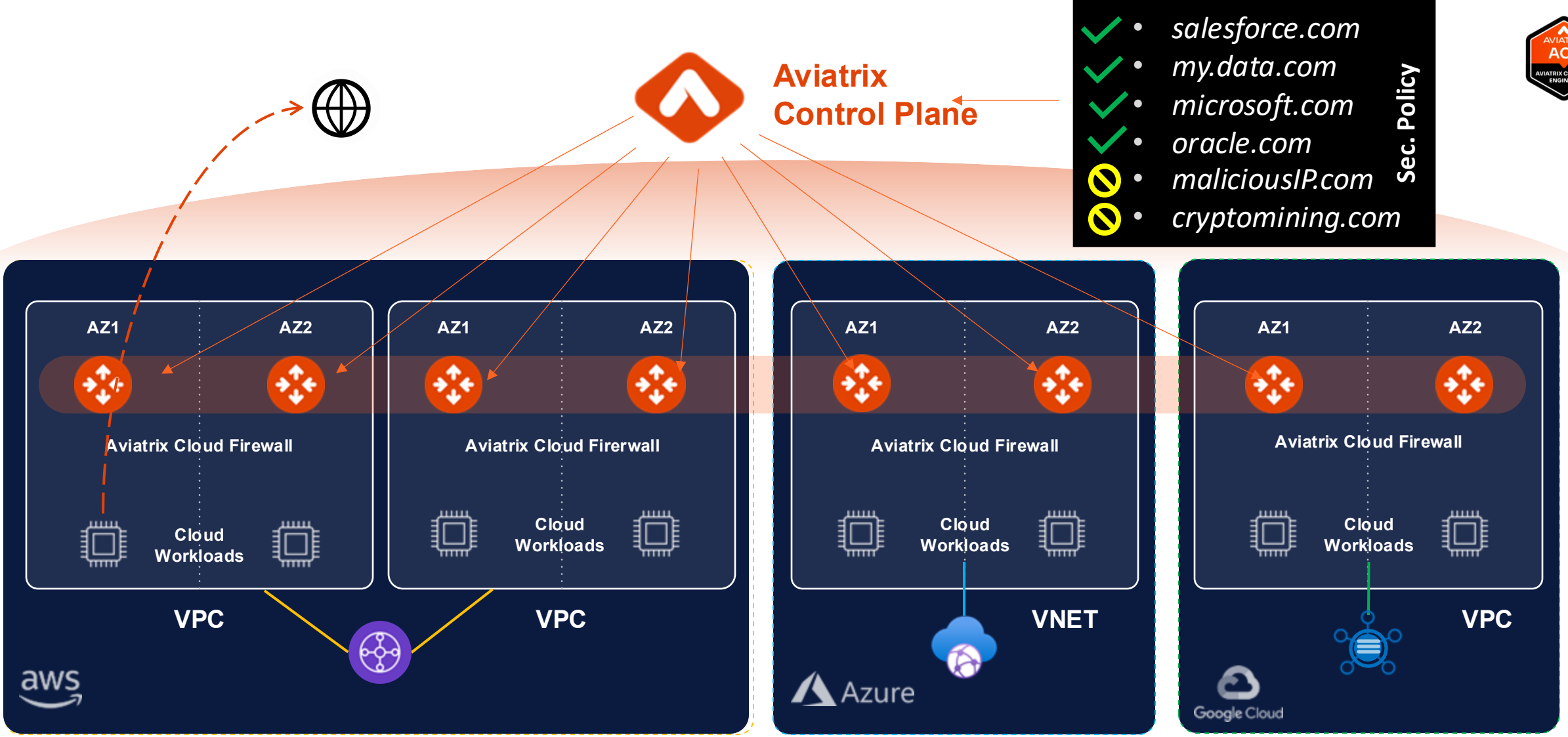
4. Centralized 3rd Party Firewall w/ Hub-and-Spoke

Challenges

- Firewalls not built for cloud: Operational complexity
- Cloud Ops < > Sec Ops Friction
- No centralized network & security intelligence
- Additional troubleshooting issues
- Not multi-cloud deployable



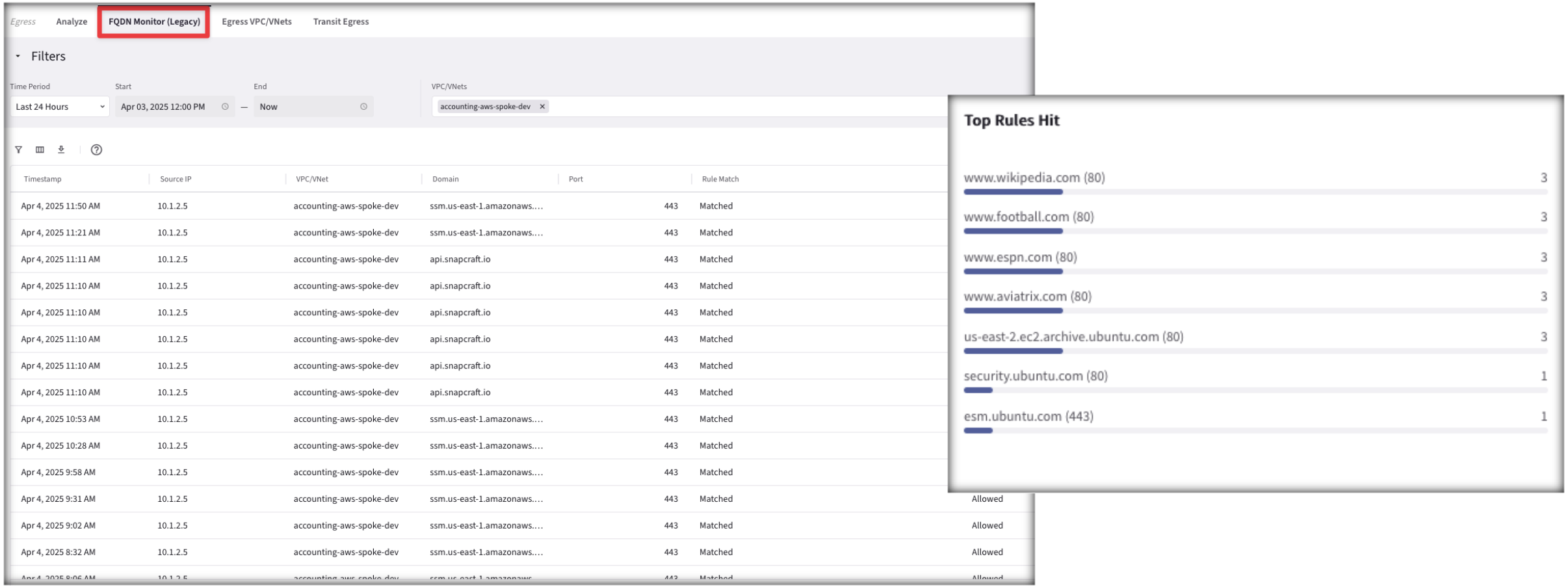
4 Centralized 3rd Party FW with Hub-and-Spoke



- Distributed Perimeter
- 1:1 Replacement of NAT GW
- Centralized Management, Visibility, and Control

Monitor

- On the **FQDN Monitor (Legacy)** section you can retrieve all the logs and therefore distinguish the domains that should be permitted from those ones that should be denied.
- Best Practice: *The Discovery Process* should be used only temporarily. As soon as you have completed your discovery, kindly proceed to activating the *Allow-List model (i.e. ZTNA approach)*.



Time Period: Last 24 Hours
Start: Apr 03, 2025 12:00 PM
End: Now
VPC/VNets: accounting-aws-spoke-dev ×

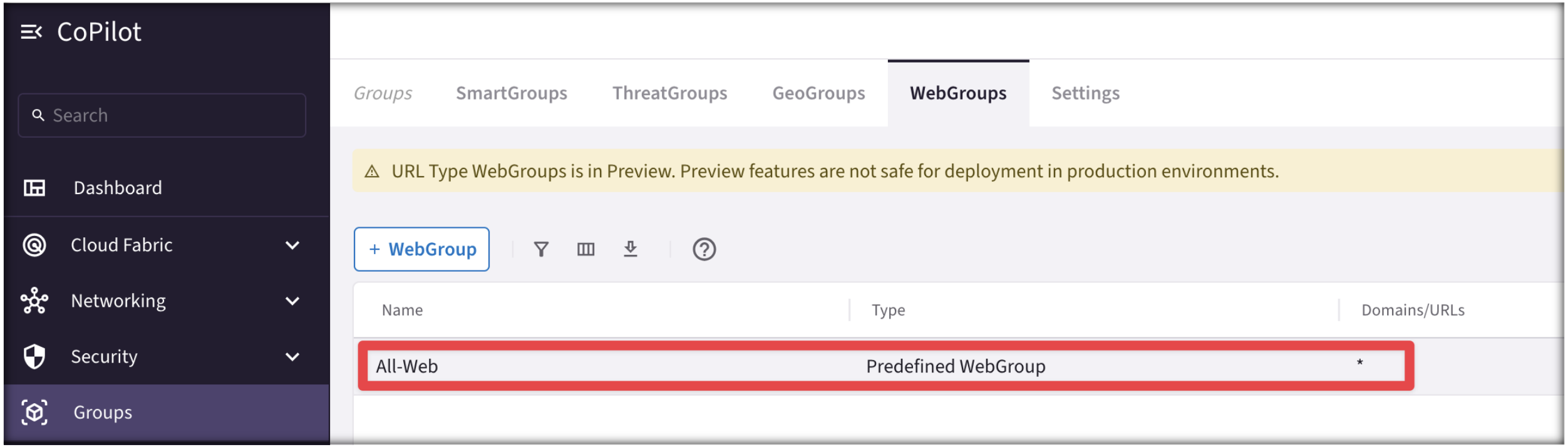
Timestamp	Source IP	VPC/VNet	Domain	Port	Rule Match	
Apr 4, 2025 11:50 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	
Apr 4, 2025 11:21 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	
Apr 4, 2025 11:11 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 11:10 AM	10.1.2.5	accounting-aws-spoke-dev	api.snapcraft.io	443	Matched	
Apr 4, 2025 10:53 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	
Apr 4, 2025 10:28 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	
Apr 4, 2025 9:58 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	
Apr 4, 2025 9:31 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	Allowed
Apr 4, 2025 9:02 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	Allowed
Apr 4, 2025 8:32 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws....	443	Matched	Allowed
Apr 4, 2025 8:06 AM	10.1.2.5	accounting-aws-spoke-dev	ssm.us-east-1.amazonaws...	443	Matched	Allowed

Top Rules Hit

www.wikipedia.com (80)	3
www.football.com (80)	3
www.espn.com (80)	3
www.aviatrix.com (80)	3
us-east-2.ec2.archive.ubuntu.com (80)	3
security.ubuntu.com (80)	1
esm.ubuntu.com (443)	1

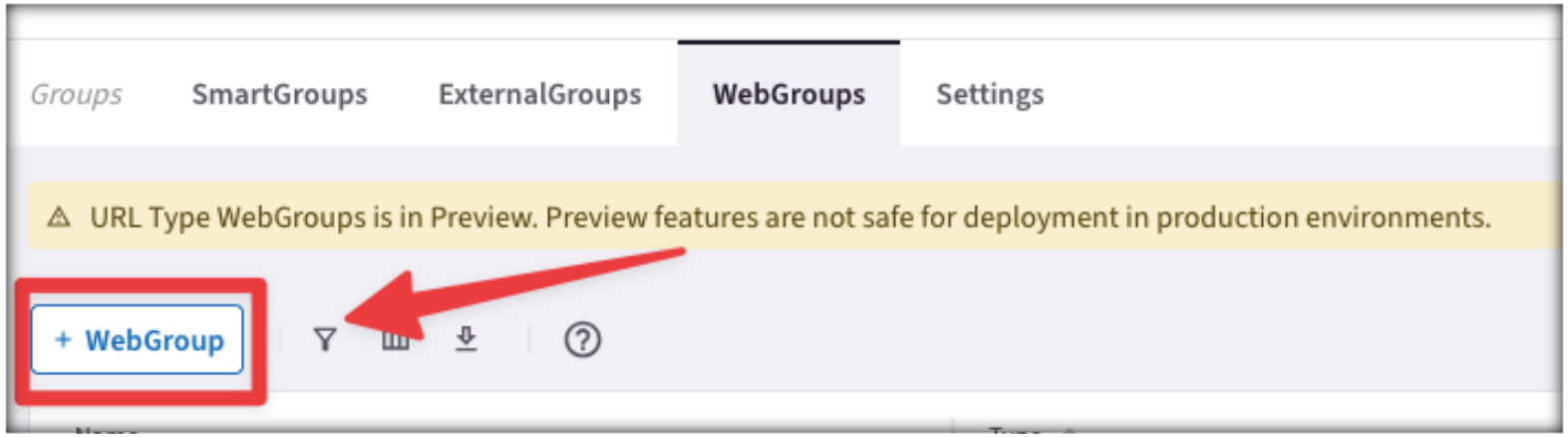
Predefined WebGroup: All-Web

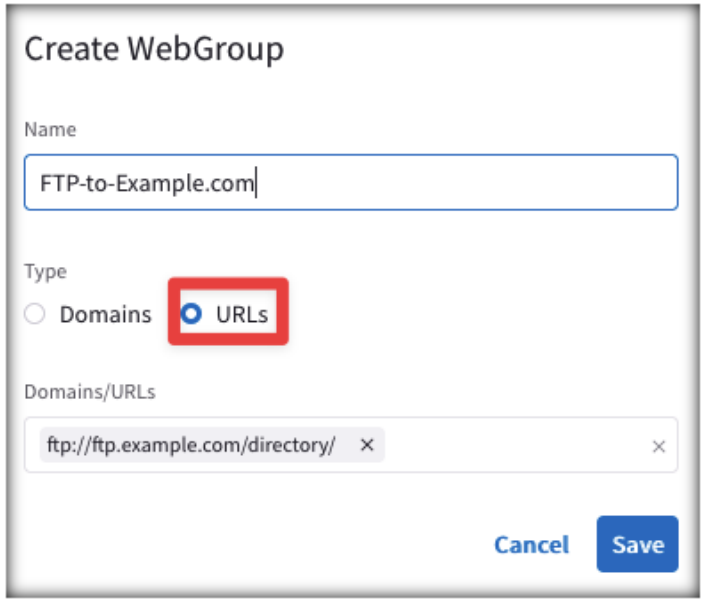
- When you navigate to **CoPilot > Groups**, a predefined WebGroup, *All-Web*, has already been created for you.
- This is an *"allow-all"* WebGroup that you must select in a Distributed Cloud Firewall rule if you do not want to limit the Internet-bound traffic for that rule, but you still want to log the FQDNs that are being accessed.

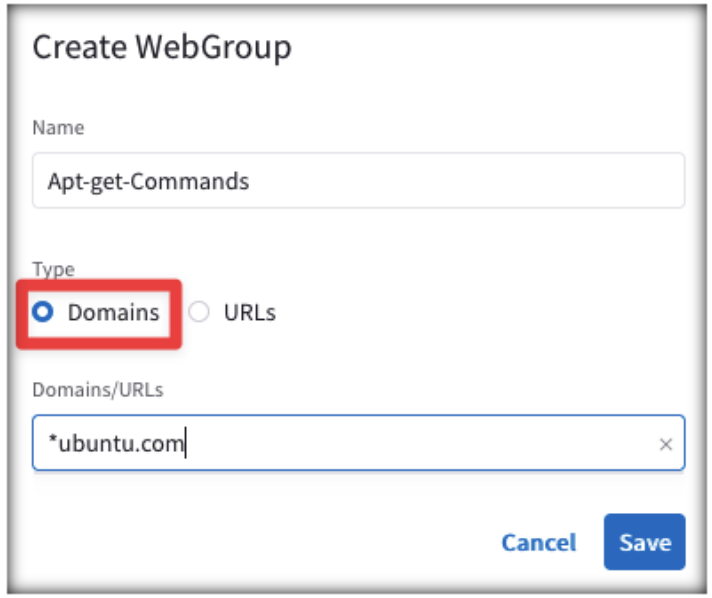


WebGroup Creation

- **WebGroups** are groupings of domains and URLs, inserted into Distributed Cloud Firewall rules, that filter (and provide security to) Internet-bound traffic.
- In addition to the predefined WebGroup ***All-Web***, you can also create two kind of custom WebGroups:
  1. **URLs WebGroup:** for HTTP/HTTPS and for other protocols, but you need to define the full Path.
     - CAVEAT: TLS Decryption must be turned on when URLs-based WebGroups are used.
  2. **Domains WebGroup:** for HTTP and HTTPS traffic (wild cards are supported – i.e. partial names).







Next: Distributed Cloud Firewall & FireNet