ENI - Elastic Network Interface
Es ist ein Service, der zu EC2 Instanzen geschaltet werden kann und bietet eine virtuelle Netzwerkkarte/Netzwerkschnittstelle. Je nachdem, was für eine EC2 Instanz benutzt wird, können mehrere Karten verwendet werden. Kann nur in der selben AZ verwendet werden.
Wie heute besprochen, “Erstellen von doppelt vernetzten Instances mit Workloads/Rollen in verschiedenen Subnetzen”.
https://docs.aws.amazon.com/de_de/AWSEC2/latest/UserGuide/scenarios-enis.html

AWS Cloud - Amazon Webservices Cloud
Ist eine Plattform für die verschiedenen Services, die Amazon anbietet. Die AWS Cloud ist eine Plattform um virtualisierte Ressourcen/Infrastruktur und für anwendungsspezifische Situationen konfigurieren zu können.
Dabei ist u.a. zu beachten, dass die AWS Cloud in verschiedene Regionen unterteilt ist.

AWS Region
AWS Region ist ein geografisch-strategisch gewählter Standort, an dem Amazon beschlossen hat, die verschiedenen Services anzubieten. Eine Region ist unterteilt in mehrere AWS Availability Zones. Geringere Latenzen durch beinahe globale Verfügbarkeit
Europe Central, South America usw.

AWS AZ
Ein AZ ist ein geografischer Standort, an dem sich mindestens 2 Datenzentren befinden sollten. (Es kann sein, dass das geändert wurde und es mittlerweile 3 AZs sein müssen.)
z.B. in Frankfurt oder Paris befinden sich mehrere Datenzentren

VPC - Virtual Private Cloud
Ist kurz gesagt ein virtualisiertes Netzwerk, in dem wir die AWS Dienste buchen und konfigurieren können - abhängig von der Anwendung, die wir anstreben.
https://aws.amazon.com/de/vpc/

Subnet
Ein Subnetz ist ein logisch isoliertes Netzwerksegment mit einem IP-Adressen-Bereich, den wir in unserer VPC definieren können. Heißt einen Bereich festlegen, in dem Geräte eine IP Adresse erhalten können.
https://docs.aws.amazon.com/de_de/vpc/latest/userguide/configure-subnets.html

Private Subnet
Ist auch ein logisch isoliertes Netzwerksegment mit einem IP-Adressen-Bereich, der nicht von der Öffentlichkeit abgerufen werden kann und ermöglicht somit nur die Kommunikation zwischen Ressourcen in der VPC. Verwendung einer privaten IP-Adresse. (Keine direkte Verbindung mit dem Internet)

Public Subnet
Genau dasselbe wie Private, nur dass hier die Kommunikation mit dem öffentlichen Netz möglich ist. Verwendung einer öffentlichen IP-Adresse.

Switch
Ist eine Hardwarekomponente im OSI-Layer 2, die Signale/Anfragen von einem Gerät über die MAC-Adresse zum jeweiligen Empfänger weiterleitet. Verbindet Geräte innerhalb eines lokalen Netzwerkes.

Router
Ist ein Gerät mit mehreren Funktionen, welche die Kommunikation zwischen Netzwerken gewährleistet.

Netzwerkinterface
Ist ein virtueller oder physischer Verbindungspunkt zwischen Geräten und einem Netzwerk. Es ermöglicht quasi die Einbindung eines Subnets über einen speziellen Port.

CIDR - Classless Inter-Domain Routing
Ist die Aufschlüsselung der IP-Adresse im 4 mal 8Bit-Muster, mit Zusatz, dass hier der Bereich für das Subnetz mit einem Slash dahinter steht.

ACL (stateless)
Access Control List ist eine Liste mit Regeln, die den Zustand der Verbindung nicht berücksichtigt. Heißt, wenn eine Verbindung für den Dateneingang genehmigt ist, muss sie für den Ausgang zusätzlich eingerichtet werden.
Zudem steuern sie den Zugriff für Netzwerke und Subnetze auf Router-Ebene.

NACL (stateless)
Network Access Control List ist auch eine Liste mit Regeln, genau wie bei ACL, müssen hier Regeln für Ein- und Ausgang definiert werden. Heißt, der Zustand der Verbindung wird hier nicht berücksichtigt.
Sie steuert die Zugriffe für Ports und IP Adressen in Subnetze

Securitygroups (statefull)
Kurz gesagt steuern sie den Datenverkehr der Instanzen innerhalb der VPC. Hier wird die Art der Verbindung berücksichtigt. Sobald eine Regel für den Eingang gesetzt wurde, erkennt die Logik, dass keine Regel für den Ausgang gesetzt sein muss.
https://docs.aws.amazon.com/de_de/vpc/latest/userguide/vpc-security-groups.html

(Stateful und Stateless sind Logiken in der Regelvergabe.)

Logging
Ist kurz gesagt ein Bericht von Ereignissen und Aktionen, die stattgefunden haben. Kann genutzt werden, um Analysen zu machen.

Im Bezug zu den Farben, weiß ich nicht, was damit gemeint ist, aber BLAU bedient sich der CIDR Schreibweise und somit die Festlegung von IP-Adressen in einem bestimmten Bereich.
GRÜN sind Hardwarekomponenten, die Daten weiterleiten, bzw. die Kommunikation zwischen Geräten und/oder Netzwerken ermöglichen.
ROT sind Sicherheitsmechanismen, die die Kommunikation zwischen Geräten und/oder Netzwerken regulieren.
Und GELB beschreibt den Zustand, den die Regeln haben können.