PART 2

1) Backdoor: EC2/Spambot:

Ec2 Instance is communicating on an unusual port 25 with a remote host.

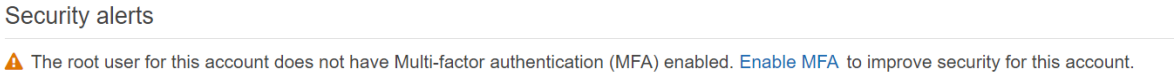
Solution:

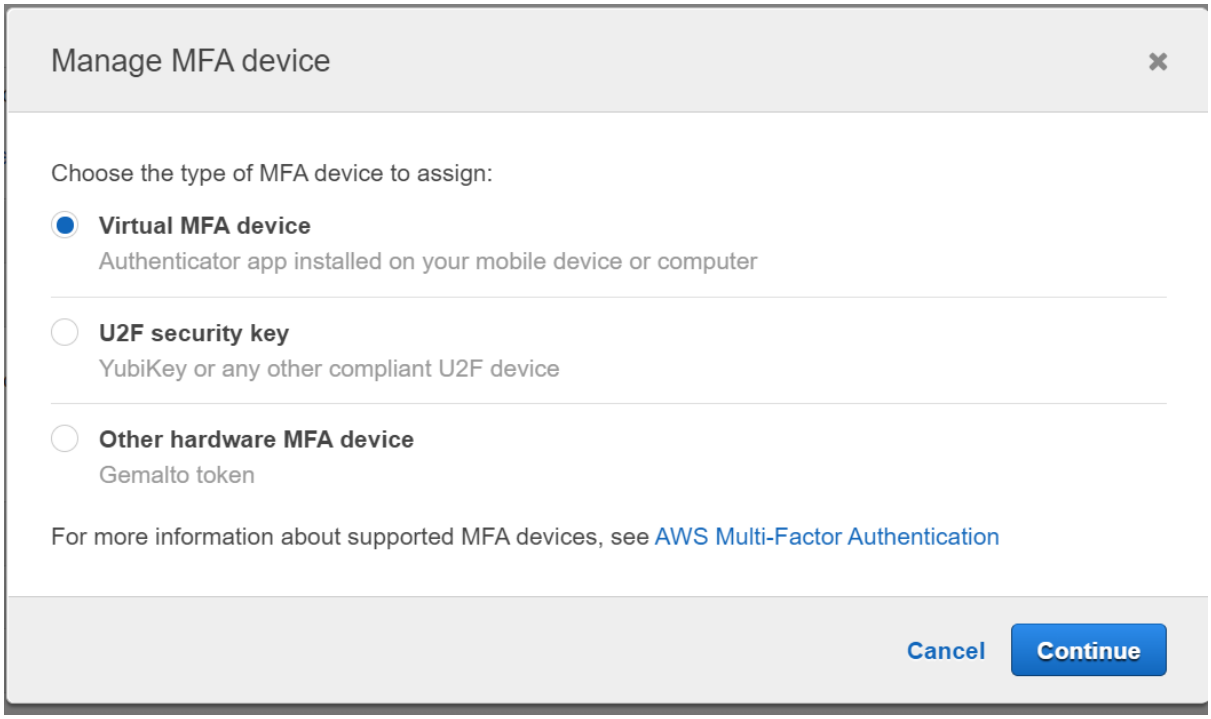
> 💡 Check Inbound rules configured in the security group attached to the EC2 Instance and remove Custom Port 25 if it is not intended.

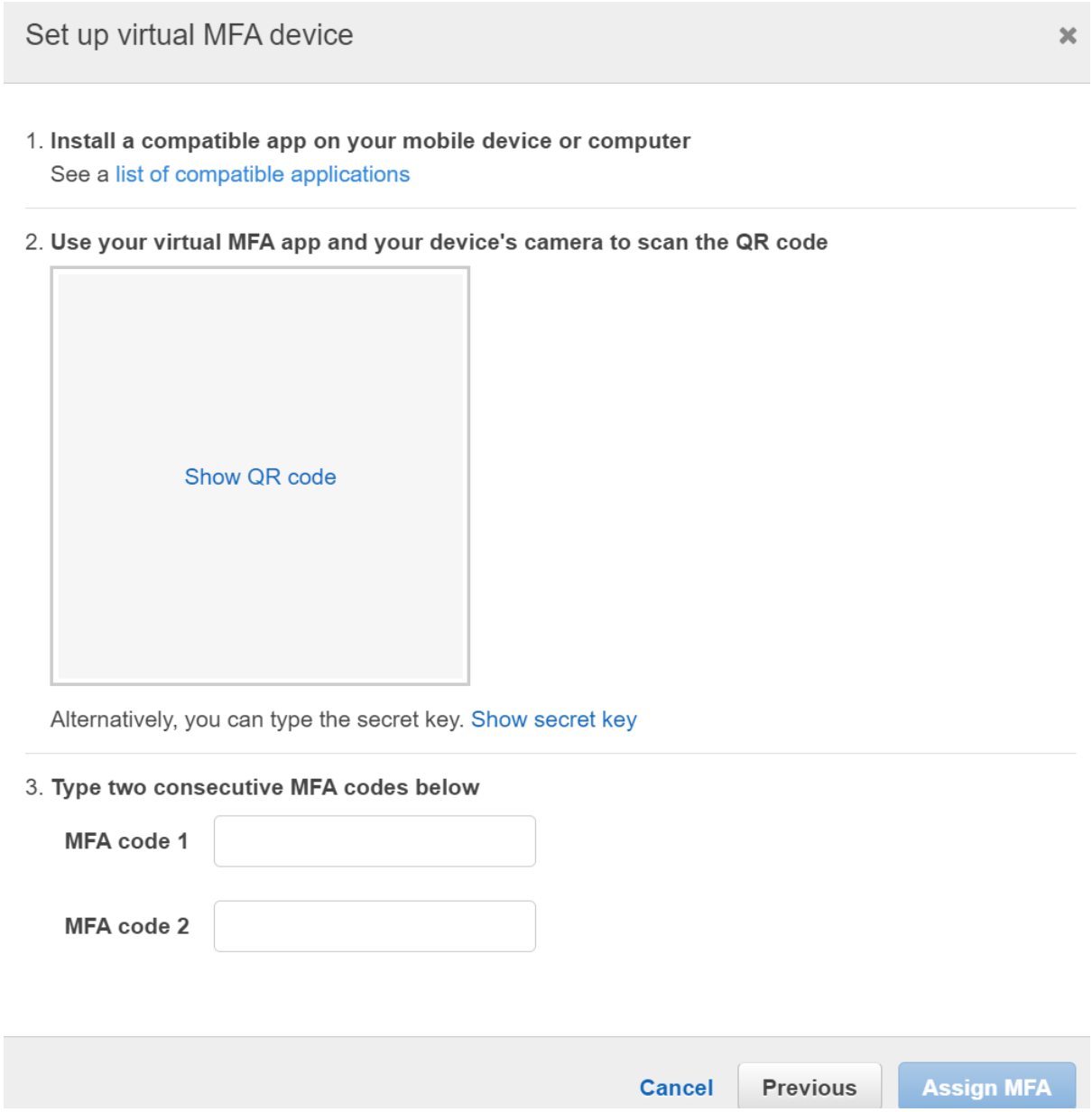
2) CloudWatch Alarm: CIS Sign-in without MFA:

Solution:

> 💡 Activate MFA for the given account using IAM Service and use Authenticators like Google Authenticator or Duo as a Primary device for MFA.




Manage MFA device
Choose the type of MFA device to assign:
Virtual MFA device
Authenticator app installed on your mobile device or computer
U2F security key
YubiKey or any other compliant U2F device
Other hardware MFA device
Gemalto token
For more information about supported MFA devices, see AWS Multi-Factor Authentication
Cancel
Continue



3) CryptoCurrency: BitCoinToolB!DNS

Solution:

> If AWS Guard Duty is signaling about the EC2 instance querying domain names related to bitcoin related activity. We can take following actions to mitigate the issues.

- Determine which domain name or IP address triggered the signal.
- Identify the process which requested the domain name or particular IP.
- Find whether it is intended or unintended for the process to query the domain name.
- Remove particular domain name or ip address from the process or application.
- Blacklist those ip addresses in firewall.