PIPELINE
ACTIONABLE CYBER THREAT DATA

Border Gateway Protocol Instructions

1.1 - BGPf configuration template - Cisco

Commented example of how to configure a BGPf session on Cisco routers and alike.

Step 1:

Select which IP you're using as nullroute target and route it to the null device. 192.0.2.1 is the usual choice here, unless you're already using it for something else

```
ip route 192.0.2.1 255.255.255.255 Null0
```

Step 2:

Depending on IOS version, you may need to configure your router for new-style community syntax.

```
ip bgp-community new-format
```

Then create labels for the communities Spamhaus is going to announce to your router. More information about the announced communities can be found here: http://www.spamhaus.org/ bgpf/

```
ip community-list standard SH-DROP permit 65190:1000
ip community-list standard SH-EDROP permit 65190:2000
ip community-list standard SH-BGPCC permit 65190:3000
```

Also create a prefix-list matching nothing. This will be used in order to avoid announcing your entire BGP routing table to Spamhaus

```
ip prefix-list NONE seq 5 deny 0.0.0.0/0
```

Step 3:

Create a route map sending every prefix matching the community Spamhaus is going to announce to the nullroute target you defined in step 1

Local-preference is set to a high value in order to override the announces you may be receiving from your upstreams.

Applying rules specific to every single community will prevent your router from nullrouting new categories Spamhaus will eventually start announcing in the future unless/until you add them manually here...

Note: We're also adding a no-export community to the received prefixes. This is already applied on Spamhaus side, but you never know...

```
route-map Spamhaus-BGPf permit 1000
description DROP
match community SH-DROP
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive route-map Spamhaus-BGPf permit 2000
description EDROP
match community SH-EDROP
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive route-map Spamhaus-BGPf permit 3000
description BGPCC
match community SH-BGPCC
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive
```

Step 4:

Finally, enter your AS number and your router's IP address.
Please ensure that you use the same IP address you have provided us in your subscription, otherwise you wont be able to peer with our feed.

Remember that, if you are not assigned with a public ASN you should choose one from the ranges reserved for private usage:

```
64512 - 65534
4200000000 - 4294967294
```

Just avoid AS65190 as this is in use by Spamhaus BGPf route servers.

For additional info please refer to https://tools.ietf.org/html/rfc6996

```
router bgp <your-AS-number>
neighbor 94.228.136.140 remote-as 65190
neighbor 94.228.136.140 description Spamhaus BGPf
neighbor 94.228.136.140 update-source
<your-routers-ip-address-or-interface> neighbor
94.228.136.140 ebgp-multihop 255
address-family ipv4 unicast
neighbor 94.228.136.140 activate
neighbor 94.228.136.140 prefix-list NONE out
neighbor 94.228.136.140 route-map Spamhaus-BGPf in
```

Additional note: On at least some platforms, the BGP handshake won't be even attempted if the session is defined as 'ebgp-multihop' and there is no explicit static route for the remote peer.

If with the above the BGP session doesn't come up, you may need to add a proper route ip route 94.228.136.140 255.255.255.255 <your-gateway>

Spamhaus BGP Sample Configuration

1.1 - BGP configuration template - Cisco

```
! Commented example of how to configure a BGPf session on Cisco routers and alike
!
! step 1:
! Select which IP you're using as nullroute target and route it to the null device. 192.0.2.1 is the usual choice here, unless you're  already using it for something else
!
ip route 192.0.2.1 255.255.255.255 Null0

! step 2:
!
! Depending on IOS version, you may need to configure your router for new-style community syntax.
!
ip bgp-community new-format
!
! Then create labels for the communities Spamhaus is going to announce  to your router. More information about the announced communities can be found here:
!http://www.spamhaus.org/bgpf/
!
ip community-list standard SH-DROP permit 65190:1000
ip community-list standard SH-EDROP permit 65190:2000
ip community-list standard SH-BGPCC permit 65190:3000
!
! Also create a prefix-list matching nothing. This will be used in order to avoid announcing your entire BGP routing table to Spamhaus
!
ip prefix-list NONE seq 5 deny 0.0.0.0/0

! step 3:
! create a route map sending every prefix matching the community SH is going to announce to the nullroute target you defined ! in step 1 local-preference is set to a high
! value in order to override the announces you may be receiving from your upstreams.
!Applying rules specific to every single community will prevent your router from nullrouting new categories Spamhaus will  eventually start announcing in the future
! unless/until you add them manually here...
!
! Note we're also adding a no-export community to the received prefixes.
! This is already applied on Spamhaus side, but you never know...
!
route-map Spamhaus-BGPf permit 1000
description DROP
match community SH-DROP
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive
route-map Spamhaus-BGPf permit 2000
description EDROP
match community SH-EDROP
set local-preference 40000
set ip next-hop 192.0.2.1

set community no-export additive
route-map Spamhaus-BGPf permit 3000
description BGPCC
match community SH-BGPCC
set local-preference 40000
set ip next-hop 192.0.2.1
set community no-export additive

! step 4:
! finally, enter your AS number and your router' IP address.
! Please ensure that you use the same IP address you have provided us in your subscription, otherwise you wont be able to peer with our feed.
! Remember that, if you are not assigned with a public ASN you should choose one from the ranges reserved for private usage:
! 64512 - 65534
! 4200000000 - 4294967294
! Just avoid AS65190 as this is in use by Spamhaus BGPf route servers.
! For additional info please refer to https://tools.ietf.org/html/rfc6996
!
router bgp <your-AS-number>
neighbor 94.228.136.140 remote-as 65190
neighbor 94.228.136.140 description Spamhaus BGPf
neighbor 94.228.136.140 update-source <your-routers-ip-address-or-interface>
neighbor 94.228.136.140 ebgp-multihop 255
address-family ipv4 unicast
neighbor 94.228.136.140 activate
neighbor 94.228.136.140 prefix-list NONE out
neighbor 94.228.136.140 route-map Spamhaus-BGPf in

! Additional note: on at least some platforms, the BGP handshake
! won't be even attempted if the session is defined as "ebgp-multihop"
! and there is no explicit static route for the remote peer.
! If with the above the BGP session doesn't come up, you may need to
! add a proper route
! ip route 94.228.136.140 255.255.255.255 <your-gateway>
```