

Search the Support Community

[Home](#) | [Top Contributors](#) | [Expert Corner](#)



[New](#) [Account](#) [History](#) [Browse](#)

2013 > September > 26

Collin Clark's Blog

[Previous](#) | [Next](#)



# What traffic to filter in CX

Posted by [Collin Clark](#) on Sep 26, 2013 6:54:49 PM

I thought I would post my configuration for sending traffic to the CX from the ASA CLI. In talking with TAC there are two schools of thought here; create a deny ACL blocking what you do not want filtered and then put a permit at the end or create a permit ACL with what you want filtered then a deny to prevent all other traffic from being sent to the CX. The latter makes more sense to me so that is the route I go.

First I create an object group with the internal networks. In this example I'll be sending all private address spaces (per RFC1918) to CX.

```
object-group network RFC1918
  description RFC1918 Private IPv4 Address Space
  network-object 10.0.0.0 255.0.0.0
  network-object 172.16.0.0 255.240.0.0
  network-object 192.168.0.0 255.255.0.0
```

Now for the ACL. I'll be sending any traffic that has an RFC1918 source address destined to anywhere on TCP port 80 or 443 to the CX.

```
access-list ACL-CX-FILTER extended permit tcp object-group RFC1918 any eq www
access-list ACL-CX-FILTER extended permit tcp object-group RFC1918 any eq https
```

Next we create the Class Map that we will be putting in the Policy Map. We tell the Class Map to look at the ACL we just created.

```
class-map CM-CX-FILTER
match access-list ACL-CX-FILTER
```

Finally we add the Class Map to the Policy Map.

```
policy-map global_policy
...
...
class CM-CX-FILTER
  cxsc fail-open auth-proxy
```

You can also do this in PRSM, but I found that it creates a somewhat-goofy naming scheme so I prefer to do it myself. Hope it helps.

110 View s      Tags: [acl](#), [traffic](#), [filter](#), [class-map](#), [cx](#)

Average User Rating      (0 ratings)

**Collin Clark**  
Member since: Sep 17, 2009

A blog that spews technical rhetoric...

[View Collin Clark's profile](#)

**Bookmarked By (0)**

View:  ▾

No public bookmarks exist for this content.

**Recent Posts**

- [Control Plane Protection CPPr](#)
- [HTTPS decryption on the CX](#)
- [What traffic to filter in CX](#)
- [CX with no authentication](#)
- [NTP with ASA, CX and PRSM](#)
- [Crashed CDA](#)
- [Adding CX to Active Directory](#)
- [ASA CX stuck in Init](#)
- [3850 Boot Mode](#)
- [ASA-X failover on 9.x code](#)

**Incoming Links**

- [Cisco ASA 5500-X Series Next-Generation Firewalls](#)

Postings may contain unverified user-created content and change frequently. The content is provided as-is and is not warranted by Cisco.