

Search the Support Community

Home Top Contributors Expert Corner



New Account History Browse

2013 > November > 08

Collin Clark's Blog

Previous Next



Control Plane Protection CPPr

Posted by Collin Clark on Nov 8, 2013 12:24:54 PM

I was browsing through the security docs the other day and came across CPPr. For detailed info go here.

This is a feature for securing devices. I used to work for a company that adhered to DISA security standards. One of things that was a pain was restricting what interfaces could be used for management. We only wanted certain interfaces to allow management protocols. There were ways to get creative, but it's a lot easier now.

```
ROUTER#conf t
Enter configuration commands, one per line. End with CNTL/Z.
ROUTER(config)#control-plane host
ROUTER(config-cp-host)#management-interface vlan13 allow ?
beep Beep Protocol
ftp File Transfer Protocol
http HTTP Protocol
https HTTPS Protocol
snmp Simple Network Management Protocol
ssh Secure Shell Protocol
telnet Telnet Protocol
tftp Trivial File Transfer Protocol
tll Transaction Language Session Protocol
<cr>
```

We can now (easily) restrict which interfaces can use what management protocol! My only complaint is that we can't use this on loopbacks which is where most/all management protocols live.

The second part I found useful is the ability to drop packets BEFORE they hit the CPU. Nice!

First let's look to see what "daemons" are running on the router.

```
ROUTER#show control-plane host open-ports
Active internet connections (servers and established)
Prot Local Address Foreign Address Service State
tcp *:22 *:0 SSH-Server LISTEN
tcp *:23 *:0 Telnet LISTEN
udp *:123 *:0 NTP LISTEN
```

Telnet is there by default. SSH and NTP showed up once I configured them. We should disable telnet. There never really was a way to disable telnet, all we could do is not use it and configure SSH and permit it. Telnet was still running though. Even though we still can't disable telnet, this is the next best thing. First we create the class map. In this example we're dropping packets that are destined to the router for ports that are not open [match closed-ports]. That certainly makes sense. Let's also drop all telnet connects too [match port tcp 23]. Now this may be belt-and-suspenders when also configuring transport under the VTYS, but I like the idea of being able to "firewall" my control plane.

```
class-map type port-filter match-any CLOSED_PORTS
match closed-ports
match port tcp 23
```

Next we create the policy map. In the real world you probably don't want the log keyword, but it's helpful when learning stuff in the lab.

```
policy-map type port-filter FILTER_CLOSED_PORTS
class CLOSED_PORTS
drop
log
```

We apply it to the control plane and then test.

```
control-plane host
service-policy type port-filter input FILTER_CLOSED_PORTS
```

I tried to telnet from a neighboring router and I was denied. On the host router I had the following in the buffer log.

```
*Nov 8 18:33:03.089: %CP-6-TCP: DROP TCP/UDP Portfilter 192.168.100.2(47624) -> 192.168.100.1(23)
```

Awesome. One thing to note is that you may want to completely configure your router before applying this. There may be things running you were not expecting. I didn't allow DHCP and that broke my home network since my router is running DHCP 😞

48 Views Tags: router, control, plane, copp, secure, cppr

Average User Rating (1 rating)

Collin Clark Member since: Sep 17, 2009 A blog that spews technical rhetoric... View Collin Clark's profile

Bookmarked By (0) View: Everyone No public bookmarks exist for this content.

Popular Blog Posts public / internet facing ACL Control Plane Protection CPPr

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 Help closing Open Ports Edge Router-Security

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