Help with ACL on VTY?

Hi All,

Here is my topology & config:

Now I want to add another line to ACL 2 to block VTY access to NFS Server (40.0.0.2) on R1.
To accomplish this the command would be "access-list 2 deny 40.0.0.2 log"
But I've applied ACL 2 on VTY 0-15 as "In" to block vty access from 10.0.0.2. Now here I need to apply as 'out'
for 40.0.0.2.
How can I accomplish this?

Regards,
Chandu
Tags: acl

Re: Help with ACL on VTY?

Chandu,
Help with ACL on VTY?

Access-class is applied on VTY lines. This is how I blocked the access to a router on the vty line
R2(config)#access-list 10 deny 10.0.0.1 log
R2(config)#line vty 0 4
R2(config-line)#access-class 10 in

R3#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Connection refused by remote host

Since its a server, I think you will have to apply it inbound on the interface f0/0 of R1, using extended ACL, by using access-group, not access-class.

---

**Re: Help with ACL on VTY?** 16 Jul, 2014 4:42 AM

↑ in response to sarah
Since its a server, I think you will have to apply it inbound on the interface f0/0 of R1, using extended ACL, by using access-group, not access-class.

>>Sarah i'm trying to restrict VTY access to 40.0.0.2 from router. I'm not trying to restrict 40.0.0.2 (server) to access the router.

*Regards,*
*Chandu*

---

**Re: Help with ACL on VTY?** 16 Jul, 2014 4:57 AM

↑ in response to Racharla Chandra Kanth

VTY lines are virtual logical connections used for management connections to routers and switches. So when you use access-class, you are applying the ACL onto a line, vty. That is fine to block managment access to a router or a switch.

Since you are trying to deny the host 10.0.0.2 from telnet-ing into 40.0.0.2, which is server, you will have to block the access to the server on the interface f0/0 inbound, while using extended ACL, as that will filter the telnet traffic.

R3(config)#access-list 101 deny tcp host 10.0.0.1 host 40.0.0.2 eq telnet
R3(config)#access-list 101 permit ip any any

And then apply it inbound using access-group

---

**Re: Help with ACL on VTY?** 16 Jul, 2014 5:14 AM

© 2016 Cisco and/or its affiliates. All Rights Reserved.  Generated on 2016-07-13-07:00
This document is Cisco Public Information.
Hi Racharla,

I guess my question here is more of the design and/or approach. The VTY lines are only resident on the routers or the network device. You are correct on using ACL’s but why apply it on the VTY line? Not sure if that's an L2 or L3 switch where 10.0.0.2 is connected to but either apply the ACL (interface or VLAN) there or on the fa0/0 of the RW.

Re: Help with ACL on VTY ? 16 Jul, 2014 5:05 AM
   ↑ in response to sarah
   ......don't take my word for it. Let's wait for the experts to clarify.

Roadcal_15 318 posts since 12 Nov, 2011
Re: Help with ACL on VTY ? 16 Jul, 2014 5:09 AM
   ↑ in response to sarah
   I agree with Sarah plus, to offload the process, in real-world, just let the NFS server block incoming telnet or ssh or whatever you want to block from 10.0.0.2.

Re: Help with ACL on VTY ? 16 Jul, 2014 5:18 AM
   ↑ in response to Roadcal_15
   Chandu,
   Since we are going to be specific with the destination as well as wanting to deny just telnet traffic, it should be placed f0/0 inbound, hence reducing unnecessary processing on the routers.
   If you use standard ACL, you can place it close to the destination, but you will end up blocking everything from 10.0.0.1-2 to 40.0.0.2 all type of traffics.

Racharla Chandra Kanth 664 posts since 2 May, 2013
Re: Help with ACL on VTY ? 16 Jul, 2014 5:25 AM
   ↑ in response to sarah
   Sarah,
   Since you are trying to deny the host 10.0.0.2 from telnet-ing into 40.0.0.2, which is server, you will have to block the access to the server on the interface f0/0 inbound, while using extended ACL, as that will filter the telnet traffic.

>>I'm not trying to do that. Ok i'll remove all the acl now.
Help with ACL on VTY?

Now what I want to do is, I want to apply an ACL to deny VTY access to 40.0.0.2 on R1. i.e. Being logged into R1 if I try to telnet into 40.0.0.2 an ACL should block it.

So I’m creating the below acl.

```
access-list 40 deny 40.0.0.2 0.0.0.0 log
access-list 40 permit any
```

Now applying it to vty 0 15

```
R1(config)#line vty 0 15
R1(config-line)#access-class 40 out
```

Now R1 should not be able to telnet to 40.0.0.2. But it is still happening.

```
R1#telnet 40.0.0.2
Trying 40.0.0.2 ... Open
```

Regards,
Chandu

---

**Racharla Chandra Kanth 664 posts since 2 May, 2013**

**Re: Help with ACL on VTY?** 16 Jul, 2014 5:28 AM

If you use standard ACL, you can place it close to the destination, but you will end up blocking everything from 10.0.0.1-2 to 40.0.0.2 all type of traffics.

>> But the book I’m studying says this:

> As you will see in the next section, you can also use extended ACLs to restrict access to the IOS device, but this configuration is much more complex. Second, extended ACLs are applied to interfaces and thus won’t be able to restrict telnet access from the router to a remote destination. And third, whenever you apply an ACL to an interface on the router, you’ll affect the performance of the router on that interface. Depending on the router model, the IOS version, and the features you have enabled, the degradation in performance will vary (today’s most current IOS versions take very little of a performance hit when using ACLs on interfaces). Therefore, if you only want to restrict telnet or SSH access to or from the router, using a standard ACL and the access-class statement on your VTYs is the best approach.
Help with ACL on VTY?

sarah 3,612 posts since 12 Sep, 2013

Chandu,
On the move, haven't tried this. VTY lines are for access to the routers from an external device.
You want to prevent (hope I'm understanding it right this time) R1 into telnet-ing into 40.0.0.2, which is a server.
That means the traffic that you're trying to block, is locally generated from within the router. You cannot apply
ACL to traffic generated by the router itself.
Roadcal_15 or someone else would have to weigh in on this. I'm not sure.
Also as he suggested

I agree with Sarah plus, to offload the process, in real-world, just let the NFS server block
incoming telnet or ssh or whatever you want to block from 10.0.0.2.

Regarding the second part, yes true, standard and access-class, but for VTY lines which are applicable to
network devices only. (I think)

Roadcal_15 318 posts since 12 Nov, 2011
Re: Help with ACL on VTY? 16 Jul, 2014 6:03 AM

You shouldn't be applying the ACL on the VTY lines Racharla. Just think of that as an ingress management
pathway. Now, from R1, since your goal is to block 10.0.0.2 from reaching 40.0.0.2 through telnet, then apply
an ACL on the ingress interface which is fa0/0. However, if you also don't want your router to have telnet
access to your NFS server, I would say, either apply another ACL on the egress interface which is f0/1 (Just
for your router) or just use one ACL on the egress interface blocking off 10.0.0.2 and your router. I hope I didn't
lose you. I also want to convey that for applying ACL's, the best practice is to apply it "inbound". This is to save
your router or network device from wasteful processing.

The way I see it and this is what's good about our profession is that you have tons of options, it's up to you on
how you incorporate or design it to your network. I hope I was able to clear the thing with the VTY lines and
where you apply your ACL's when trying to allow and/or block entities. For additional reading, I can recommend
The Network Warrior (2nd Ed) by Mr. Donahue. It's a great read.

sarah 3,612 posts since 12 Sep, 2013
Re: Help with ACL on VTY? 16 Jul, 2014 6:44 AM

Roadcal_15,
Help with ACL on VTY?

However, if you also don't want your router to have telnet access to your NFS server, I would say, either apply another ACL on the egress interface which is f0/1 (Just for your router)

I'm probably not understanding it right here, hence just clarifying. If you're saying that applying ACL outbound on f0/1, will block the router itself from telnet-ing into 40.0.0.2, I think it won't. Because the packets are generated by the router itself.

R1(config)#access-list 101 deny tcp any host 40.0.0.2 eq telnet
R1(config)#access-list 101 permit ip any any
R1(config)#int f0/1
R1(config-if)#ip access-group 101 out
R1#show ip interface f0/1
FastEthernet1/0 is up, line protocol is up
  Internet address is 40.0.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled

Outgoing access list is 101

Inbound  access list is not set

R1#telnet 40.0.0.2
Trying 40.0.0.2 ... Open

User Access Verification

Username:
At the same time, If I try to telnet from 10.0.0.2 (R3, configured as host)

R3#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Destination unreachable; gateway or host down

It worked, I was able to block telnet here from 10.0.0.2 to 40.0.0.2

R1#
*Mar  1 02:34:29.299: IP: tableid=0, s=10.0.0.2 (FastEthernet2/0), d=40.0.0.2 (FastEthernet0/1), routed via FIB
*Mar  1 02:34:29.299: IP: s=10.0.0.2 (FastEthernet2/0), d=40.0.0.2 (FastEthernet0/1), len 44, access denied
*Mar  1 02:34:29.303: TCP src=53895, dst=23, seq=2985041040, ack=0, win=4128 SYN
---omitted----
Help with ACL on VTY?

*Mar 1 02:34:29.307: ICMP type=3, code=13

The outbound ACL configured on f0/1, will not block the packets generated by the router itself. However when I tried to telnet into 40.0.0.2 from 10.0.0.2, I couldn't because of the ACL configured on f0/1, outbound. So the transit traffic will be blocked, though not what's generated by the router itself. Hence the router would be able to telnet.

Navneet.Gaur 1,684 posts since 22 Mar, 2010

Re: Help with ACL on VTY? 16 Jul, 2014 7:37 AM

Hi Racharla Chandra Kanth.

In context to post #2

Racharla Chandra Kanth wrote:

i'm trying to restrict VTY access to 40.0.0.2 from router. I'm not trying to restrict 40.0.0.2 (server) to access the router.

1. There are a few ways to achieve what you are trying to do, block telnet access from R1 to 40.0.0.2.

2. But first you have to keep in mind that you are trying to "restrict" locally generated requests from the router R1.

3. You could deny the return telnet traffic from 40.0.0.2 to the router R1.

R1

ip access-list extended deny-return-telnet
deny tcp host 40.0.0.2 eq 23 host 40.0.0.254
permit ip any any

interface FastEthernet 0/1
ip access-group deny-return-telnet in
end

4. As stated earlier, you could deny incoming telnet traffic on 40.0.0.2 it-self as well.

5. Lastly you can use local policy to divert the outgoing telnet traffic from R1 to 40.0.0.2 to a null 0 interface, on R1. The document below sites another example:

https://learningnetwork.cisco.com/docs/DOC-24244
Help with ACL on VTY?

R1
configure terminal
ip access-list extended deny-local-telnet
permit tcp host 40.0.0.254 host 40.0.0.2 eq 23
exit

route-map deny-local-telnet
match ip address deny-local-telnet
set interface null 0
exit

ip local policy route-map deny-local-telnet
end

Take care,
Navneet.

----------
Update:
• Point #5 above, is not within the scope of CCNA
• I have included it only as a point of reference, so that you are aware of the possibilities and understand that normal access control lists, do not monitor locally generated traffic within a router, under *normal and standard configuration

Navneet.Gaur  1,684 posts since 22 Mar, 2010
Hi Racharla Chandra Kant.

1. You are already be aware of the way access lists work. The following post #8 might help you consolidate your understanding further.

https://learningnetwork.cisco.com/message/410363#410363

2. Go through the post #12 of the link provided within that post as well. Maybe it will help.

Take care,
Navneet.

----------
Update:
Help with ACL on VTY?

There are a couple of existing discussions that may be of additional help as well:
https://learningnetwork.cisco.com/message/250059#250059
https://learningnetwork.cisco.com/message/368358#368358

Richard Burts 302 posts since 14 Jan, 2009

I am not clear what was the intention of the original post but it seemed to me that it was to prevent access from the router to the server. In that case there is a simple solution which is to configure an additional standard access list similar to access-list 2 which denies the host address of the server and then to apply this as access-class out.

We tend to think of access-class in terms of its use to limit access TO the router/switch. But it also is effective in limiting access from the router to other resources.

HTH

Rick

sarah 3,612 posts since 12 Sep, 2013

Richard Burts...thanks for clearing that! I could have gone on and on...

Richard Burts 302 posts since 14 Jan, 2009

Having read through the discussion again I see that somehow I missed post #8 where Chandu says that he tried what I suggested and that it did not work. I am surprised at that and believe that it should have worked. Perhaps some additional detail might help us understand why it did not work.

HTH

Rick

Navneet.Gaur 1,684 posts since 22 Mar, 2010
Re: Help with ACL on VTY? 16 Jul, 2014 9:59 AM

Hi Richard Burts.
Help with ACL on VTY?

1. There is an interesting article by Paul Stewart regarding "access-class x out".

http://www.packetu.com/2011/06/15/the-elusive-access-class-out-command/

2. Basically "access-class x out" will apply
   • if, from within an existing vty session from another router to R1
   • a new telnet connection is initiated

Take care,
Navneet.

Richard Burts 302 posts since 14 Jan, 2009
Re: Help with ACL on VTY? 16 Jul, 2014 9:57 AM

That is an interesting article and it does suggest a possible reason why the attempt shown by Chandu did not work - if his session on R1 was a console session then the access class applied to the vty would not work.

HTH

Rick

Navneet.Gaur 1,684 posts since 22 Mar, 2010
Re: Help with ACL on VTY? 16 Jul, 2014 10:14 AM

Hi Richard Burts.

1. You helped me out once regarding post edits.
   https://learningnetwork.cisco.com/message/351041#351041

2. I kind of "helped" with this "access-class x out"

3. Now we are even!

Take care,
Navneet.

---------
Help with ACL on VTY?

Update:
Of course, that is supposed to be taken in lighter vein!

Richard Burts 302 posts since 14 Jan, 2009

Re: Help with ACL on VTY? 16 Jul, 2014 10:23 AM

in response to Navneet.Gaur

Navneet

Yes that was also an interesting discussion and I am glad that my response was helpful to you. Your response in this discussion was helpful to me. So I am glad to be even and I am glad to see your continued activity in the forum.

HTH

Rick

Navneet.Gaur 1,684 posts since 22 Mar, 2010

Re: Help with ACL on VTY? 16 Jul, 2014 10:30 AM

in response to Richard Burts

Hi Richard Burts.

1. I do hope you are taking it in the lighter vein that it was intended as.

2. It has been pointed out to me by one of the members that the way you site real life examples from your work makes your replies more meaningful, interesting and noteworthy.

3. So, your participation is also very much appreciated as well.

Take care,

Navneet.

Roadcal_15 318 posts since 12 Nov, 2011

Re: Help with ACL on VTY? 16 Jul, 2014 10:48 AM

in response to sarah

Sorry for not expounding on that one sarah. Went ahead and isolated Racharla's lab. with the simple ACL he created, he can basically block telnet session from 10.0.0.2 to 10.0.0.254, 40.0.0.254 and 40.0.0.2 if he applies the same ACL on the VTY lines and on fa0/1.

ON R1:
Help with ACL on VTY?

access-list 1 deny 10.0.0.2 log
access-list 1 permit any log

line vty 0 4
access-class 1 in
password racha
login
line vty 5 15
access-class 1 in
password racha
login

interface FastEthernet0/1
ip address 40.0.0.254 255.255.255.0
ip access-group 1 out
duplex auto
speed auto
end

On PC2, he will basically get:

PC2#telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host

PC2#telnet 40.0.0.254
Trying 40.0.0.254 ...
% Connection refused by remote host

PC2#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Destination unreachable; gateway or host down

This basically solves Racharla's issue with 10.0.0.2. Now, tell us Racharla if you basically want to stop here?
Help with ACL on VTY?

If you still want to further isolate your NFSServer even from your default gateway. Then, a bit of logic needs to be applied. You have to see the common point and the limitations you have. So what Mr. Gaur suggested is correct (Thank you sir!), he stated to block the traffic that's coming from the common source, which is your NFSServer. So here's what I did.

ON R1:
!
access-list 1 deny 10.0.0.2 log
access-list 1 permit any log
!
access-list 100 deny tcp host 40.0.0.2 eq telnet host 10.0.0.2
access-list 100 deny tcp host 40.0.0.2 eq telnet host 10.0.0.254
access-list 100 deny tcp host 40.0.0.2 eq telnet host 40.0.0.254
access-list 100 permit ip any any log
!
line vty 0 4
access-class 1 in
password racha
login
!
line vty 5 15
access-class 1 in
password racha
login
!
interface FastEthernet0/1
ip address 40.0.0.254 255.255.255.0
ip access-group 100 in
duplex auto
speed auto
!

ON PC2, here are the results:

PC2#telnet 10.0.0.254
Trying 10.0.0.254 ...
% Connection refused by remote host

PC2#telnet 40.0.0.254
Help with ACL on VTY?

Trying 40.0.0.254 ...
% Connection refused by remote host

PC2#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Connection timed out; remote host not responding

AND ON ROUTER1:
R1#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Connection timed out; remote host not responding

Hope this helps you out buddy and thank you for giving us a challenge. How simple or hard it may be, you still learn stuff along the way. Finding the answer is good but creating solutions is much better. Good luck on your studies!

Thank you Sarah and Navneet as well!

---

Navneet.Gaur 1,684 posts since 22 Mar, 2010
Re: Help with ACL on VTY? 16 Jul, 2014 10:49 AM

Hi Roadcal_15.

↑ in response to Roadcal_15
Help with ACL on VTY?

1. It is always a pleasure.

Take care,
Navneet.

sarah 3,612 posts since 12 Sep, 2013
Re: Help with ACL on VTY? 16 Jul, 2014 11:02 AM

Roadcal_15,

Instead we should be thanking you!! That was a very professional response there and so easily explained effortlessly by you, in few words....yet so precise.

Richard, thank you too.

Racharla Chandra Kanth 664 posts since 2 May, 2013
Re: Help with ACL on VTY? 16 Jul, 2014 10:42 PM

Thanks Everyone.

I understood that my acl was not working because i was into router with console.
Now if i telnet into R1 and try to telnet to 40.0.0.2 it doesn't work.

PC2#telnet 10.0.0.254
Trying 10.0.0.254 ... Open

User Access Verification

Password:
R1>telnet 40.0.0.2
Trying 40.0.0.2 ...
% Connections to that host not permitted from this terminal
R1>

And to restrict access from R1 to 40.0.0.2, i did:
line con 0
access-class 40 out

R1#show access-list
Standard IP access list 40
  10 deny 40.0.0.2 log (3 matches)
Help with ACL on VTY?

20 permit any
R1#

Now from R1 via console:
R1#telnet 40.0.0.2
Trying 40.0.0.2 ...
% Connections to that host not permitted from this terminal
R1#

Thanks all again. And Navneet the links were of great help.

Regards,
Chandu

Navneet.Gaur 1,684 posts since 22 Mar, 2010
Re: Help with ACL on VTY? 17 Jul, 2014 12:16 AM
in response to Racharla Chandra Kanth
1. It is always a pleasure Chandu.

2. "Access-class x out" on a consol line, instead of a vty, as explained by Paul Stewart, is an effective solution as well, if access limitation only from a direct consol session is required.

3. In contrast, local policy will limit access, from both, consol as well as vty, if connection is initiated from within the router.

Take care,
Navneet.

----------
Update:
Of course both line vty and consol can have "access-class x out" applied individually for a *similar effect, as you have done in the post preceding this one.
1 2 Previous Next