Setting method_②Restrict access to the NetScaler interface (SNIP)

Setting method via GUI

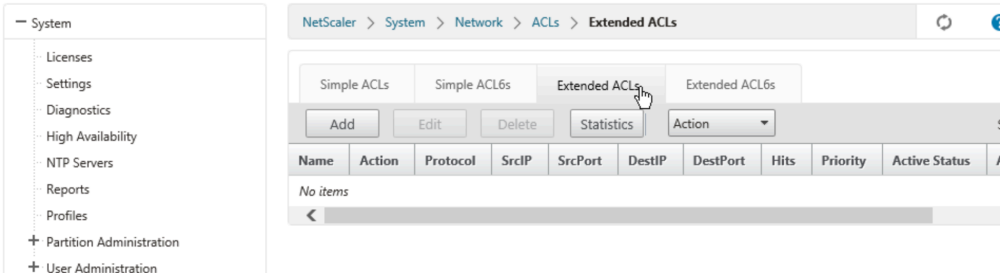
Setting method in case of logging in to NetScaler via http or https is as follows.

Move to setting scrren of ACL

Click System>Networks>ACLs and click "Extended ACLs" from tab.

Example below shows there is no existing ACL setting.

Following procedure is displayed on the basis that there is no existing ACL setting.



Add ACL setting

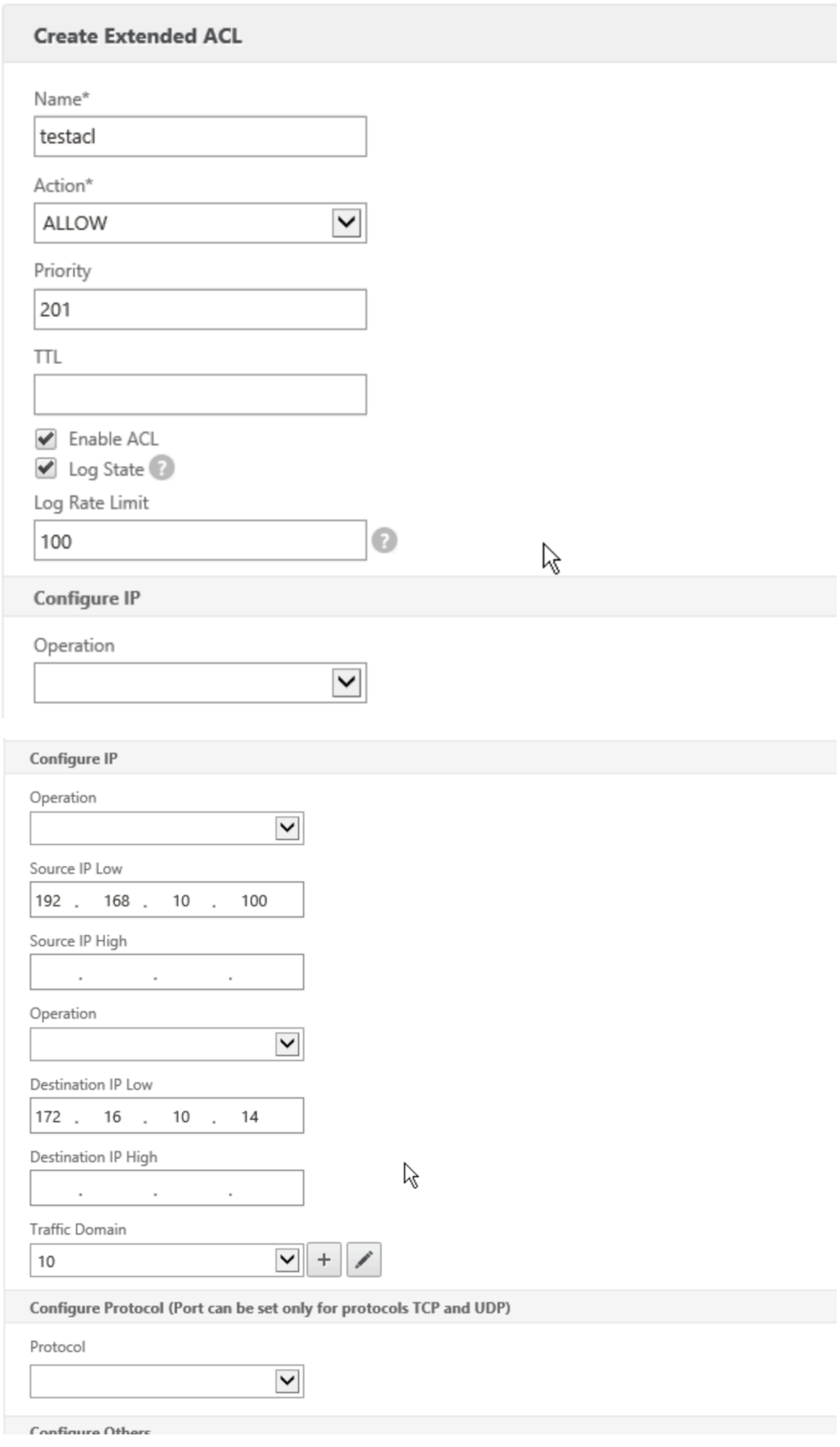
Click [Add] and open setting screen. 。

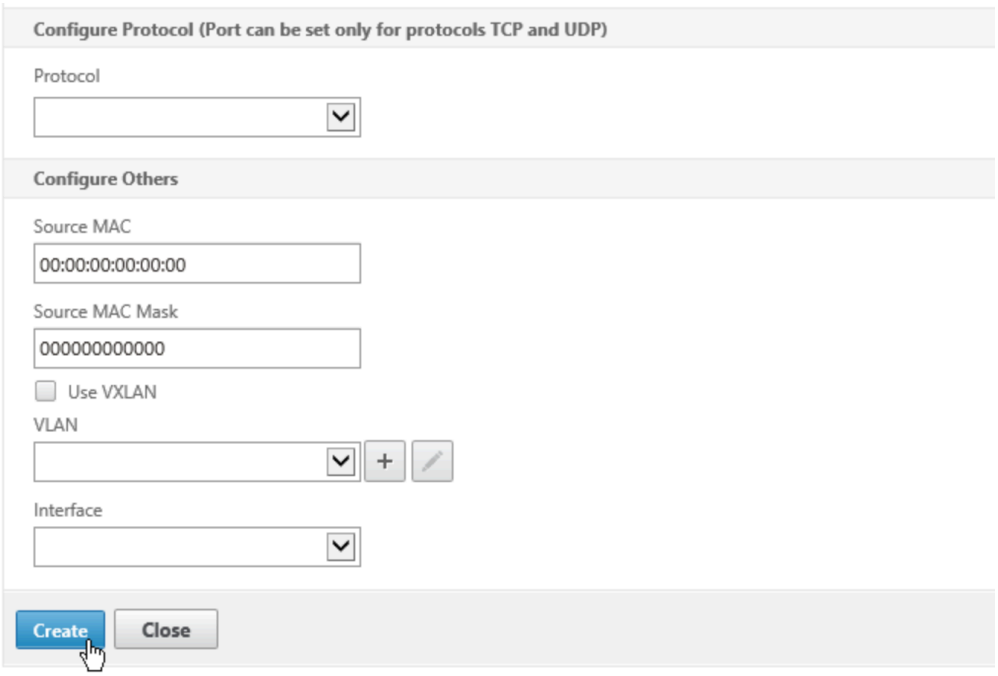
Set allow or deny access according to the customers' designs.

Please refer to documents below provided by Citrix for details of ACL settings.

- NetScaler VPX 11.0
  - https://docs.citrix.com/en-us/netscaler/11/networking/access-control-lists-acls.html
- NetScaler VPX 10.5
  - https://docs.citrix.com/en-us/netscaler/10-5/ns-nw-gen-wrapper-10-con/ns-nw-acl-intro-wrapper-con.html

Example below shows access from 192.168.10.100 is allowed on SNIP（172.16.10.14） which is able to access for management.


Create Extended ACL
Name*
testacl
Action*
ALLOW
Priority
201
TTL
Enable ACL
Log State
Log Rate Limit
100
Configure IP
Operation
Configure IP
Operation
Source IP Low
192 . 168 . 10 . 100
Source IP High
Operation
Destination IP Low
172 . 16 . 10 . 14
Destination IP High
Traffic Domain
10
Configure Protocol (Port can be set only for protocols TCP and UDP)
Protocol



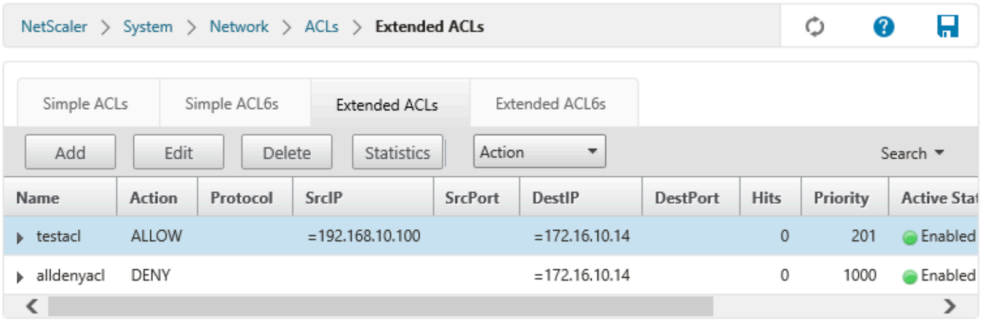
> ⚠ Priority of Access Control List and / or Policy-Based Routing can be utilized from 200th number (1st through 199th are not available).
>
> Refference： Restrictions of Service Description
>
> - https://ecl.ntt.com/en/documents/service-descriptions/rsts/network/loadbalancer.html#id25

Confirm ACL settings

Confirm ACL settings customers set on purpose is shown on ACLs screen.

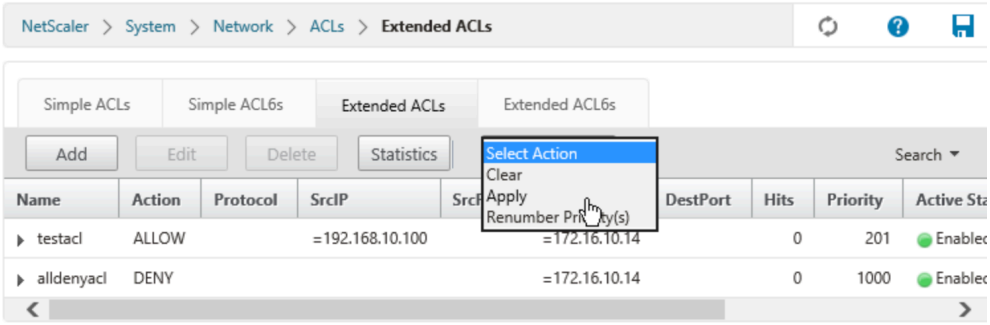
Example below shows two ACL settings which allows access only from 192.168.10.100 on SNIP（172.16.10.14） able to access for management are displayed.

- testacl
  - Allow access which DestinationIP is 172.16.10.14 and SourceIP is 192.168.10.100（priority201）
- alldenyacl
  - Deny access which DestinationIP is 172.16.10.14（priority1000）



Apply ACL settings

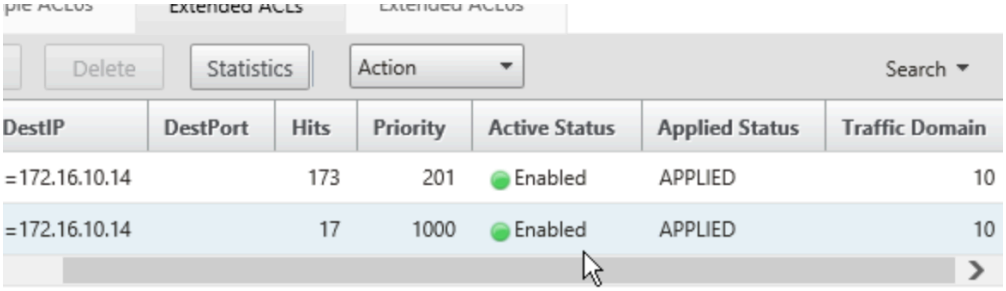
Select "Action" and click "Apply" from pull-down.



Pop up box is displayed, and click [Yes].

Confirm Restriction access1

Scroll to the right, and confirm "Applied Status" shows APPLIED.



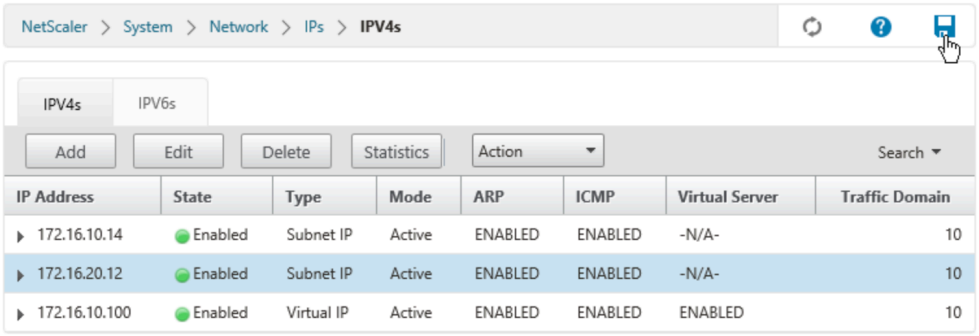
Confirm Restriction access2

Login to SNIP which access is restricted from outside of NetScaler via ssh and gui(http,https), and acquire value via snmp. Confirm access is available from specified one..

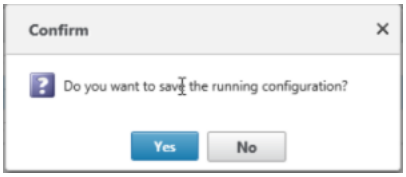
Examples are not shown because it depends on customers' environment.

Save settings

Click Floppy disk mark which is shown at upper right of screen.



Pop up box is displayed, click [Yes].



> If above procedure is not followed, restoration to its former state occurs in case of rebooting NetScaler with some reason.
>
> Please make sure to save setting.

Setting method via CLI

Setting method in case of logging in to NetScaler via ssh is as follows.

Confirm ACL settings

```
show ns acl
```

Execute above command, and confirm existing ACL settings.

Example below shows there is no existing ACL setting.

Following procedure is displayed on the basis that there is no existing ACL setting.

```
> show ns acl
 Done
```

ACL　settings

Set allow or deny access according to the customers' designs by executing commands below.

Consider logstate option if customers want to acquire logs.

```
add ns acl "ACL名" ALLOW -srcIP=XX.XX.XX.XX -destIP=YY.YY.YY.YY -priority Z -logstate ENABLED -td 10
add ns acl "ACL名" DENY -destIP=YY.YY.YY.YY -priority ZZ -td 10
```

Please refer to documents below provided by Citrix for details of ACL settings.

- NetScaler VPX 11.0
  - https://docs.citrix.com/en-us/netscaler/11/networking/access-control-lists-acls.html
- NetScaler VPX 10.5
  - https://docs.citrix.com/en-us/netscaler/10-5/ns-nw-gen-wrapper-10-con/ns-nw-acl-intro-wrapper-con.html

Example below shows access from 192.168.10.100 is allowed on SNIP（172.16.10.14） which is able to access for management.

```
> add ns acl testacl ALLOW -srcIP = 192.168.10.100 -destIP = 172.16.10.14 -priority 201 -logstate ENABLED
-td 10
 Done
> add ns acl alldenyacl DENY -destIP = 172.16.10.14 -priority 1000 -td 10
 Done
```

⚠ Priority of Access Control List and / or Policy-Based Routing can be utilized from 200th number (1st through 199th are not available).

Refference： Restrictions of Service Description

https://ecl.ntt.com/en/documents/service-descriptions/rsts/network/loadbalancer.html#id25

Confirm ACL setting

```
show ns acl
```

Execute above command, and confirm ACL setting which customers set on purpose is set in the status of NOTAPPLIED.

Example below shows Applied Status of two ACL settings are NOTAPPLIED.

```
> show ns acl
1) Name: testacl
 Action: ALLOW                    Hits: 0
 srcIP = 192.168.10.100
 destIP = 172.16.10.14
 srcMac:
 Protocol:
 Vlan:                      Interface:
 Active Status: ENABLED           Applied Status: NOTAPPLIED
 Priority: 201                NAT: NO
 TTL:
 Log Status: ENABLED              Log Rate limit: 100
 Forward Session: NO
 Traffic Domain: 10
2) Name: alldenyacl
 Action: DENY                     Hits: 0
 srcIP
 destIP = 172.16.10.14
 srcMac:
 Protocol:
 Vlan:                      Interface:
 Active Status: ENABLED           Applied Status: NOTAPPLIED
 Priority: 1000               NAT: NO
 TTL:
 Log Status: DISABLED
 Forward Session: NO
 Traffic Domain: 10
 Done
```

Apply ACL setting

```
> apply ns acls
```

Execute above command, and apply settings.

Example below shows processing is completed.

```
> apply ns acls
 Done
```

Confirm Access restriction 1

```
> show ns acl
```

Execute above command, and confirm ACL settings.

Example below shows ACL setting customers set on purpose is shown and processing applies setting is completed.

```
> show ns acl
1) Name: testacl
 Action: ALLOW                  Hits: 119
 srcIP = 192.168.10.100
 destIP = 172.16.10.14
 srcMac:                        srcMacMask: 000000000000
 Protocol:
 Vlan:                          Interface:
 Active Status: ENABLED         Applied Status: APPLIED
 Priority: 201                  NAT: NO
 TTL:
 Log Status: ENABLED            Log Rate limit: 100
 Forward Session: NO
 Traffic Domain: 10
2) Name: alldenyacl
 Action: DENY                   Hits: 6
 srcIP
 destIP = 172.16.10.14
 srcMac:                        srcMacMask: 000000000000
 Protocol:
 Vlan:                          Interface:
 Active Status: ENABLED         Applied Status: APPLIED
 Priority: 1000                 NAT: NO
 TTL:
 Log Status: DISABLED
 Forward Session: NO
 Traffic Domain: 10
 Done
```

Confirm Access restriction2

Login to SNIP which access is restricted from outside of NetScaler via ssh and gui(http,https), and acquire value via snmp. Confirm access is available from specified one..

Examples are not shown because it depends on customers' environment.

Save settings

```
save ns config
```

Execute above command and save settings changed.

⚠ If above procedure is not followed, restoration to its former state occurs in case of rebooting NetScaler with some reason.

Please make sure to save setting.

Revision history

Date	Version	Detail
2017/9/27	1.0.0	First edition