設定方法_②アクセス制限の実施

GUIでの設定方法

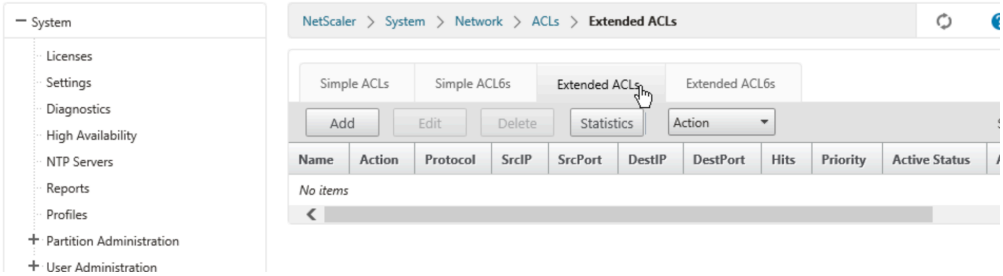
以下操作は、NetScalerに対しhttpもしくはhttpsでログインした場合の設定方法を記載します。

ACL設定画面への遷移

System>Networks>ACLsと画面遷移し、さらにタブから"Extended ACLs"を選択ください。

以下の例では、既存のACL設定がないことがわかります。

以降はACLが存在しない前提で設定変更を進めます。



ACL設定の追加

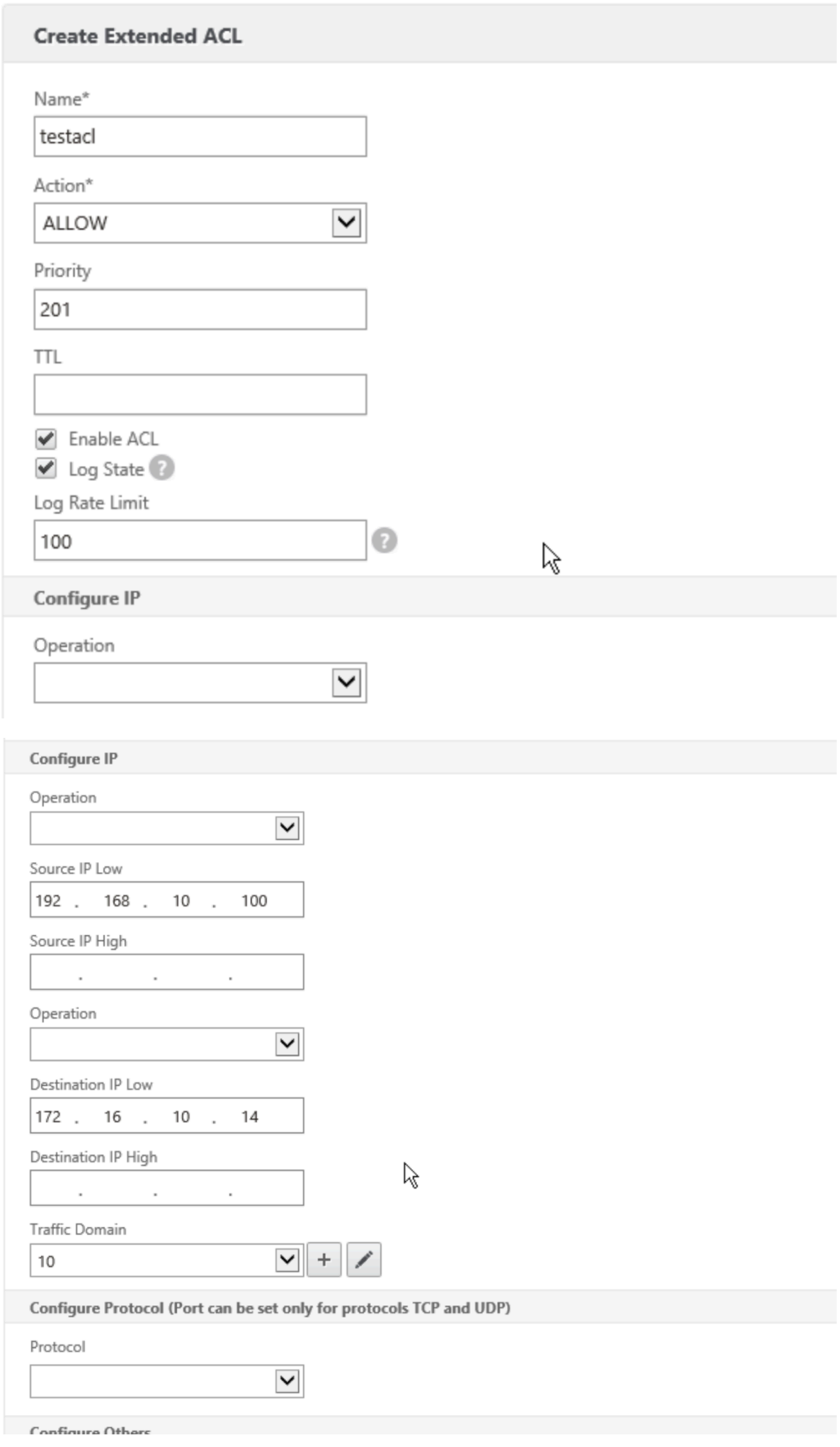
[Add]を押下し、設定画面を開きます。

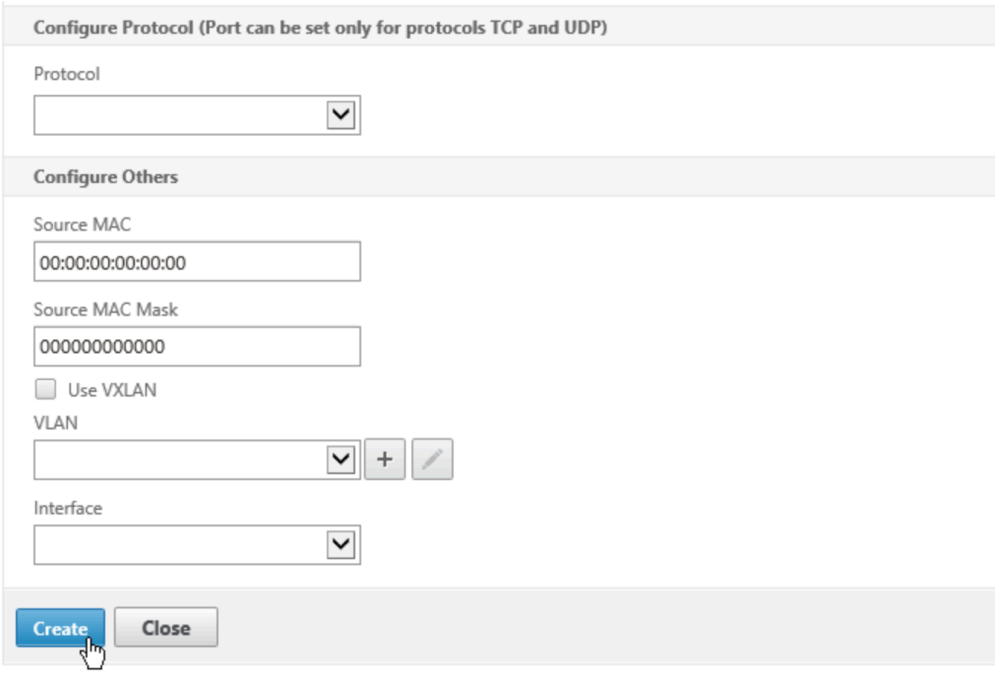
お客様の設計に合わせ許可する通信、許可しない通信を設定ください。

ACL機能に詳細につきましてはCitrix社の公式ドキュメントをご参照ください。

- 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

以下の例では管理用通信が可能なSNIP（172.16.10.14）に対して、192.168.10.100からの通信を許可する設定を入れています。


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



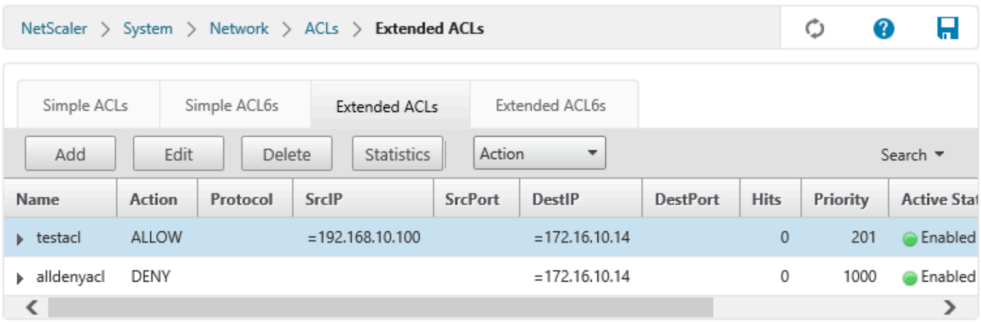
> アクセスコントロールリスト、ポリシーベースルーティングのPriorityは200番台から利用できます。（1~199は管理用として使用しているため利用できません。）
>
> 参考：サービス説明書 制約事項
>
> - https://ecl.ntt.com/documents/service-descriptions/loadbalancer/loadbalancer.html#id30

ACL設定の確認

ACLsの画面にて、意図したACL設定が入っていることを確認します。

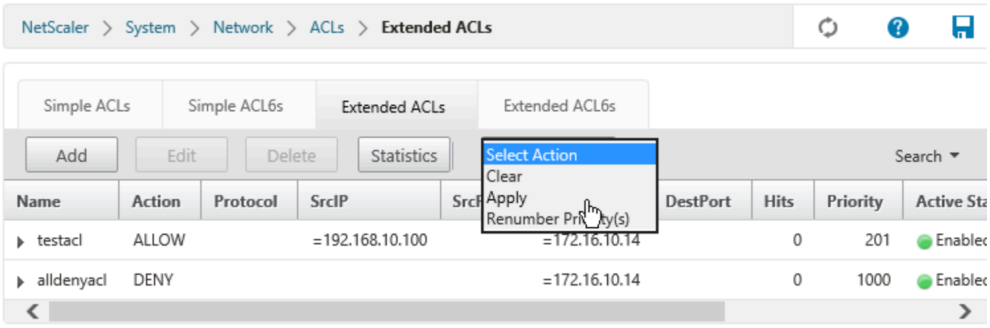
以下の例は管理用通信が可能なSNIP（172.16.10.14）に対し192.168.10.100からの通信のみを許可するための２行のACL設定が入っています。

- testacl
  - DestinationIPが172.16.10.14で、SourceIPが192.168.10.100の通信を許可する（priority201）
- alldenyacl
  - DestinationIPが172.16.10.14の通信を許可しない（priority1000）



ACL設定の適用

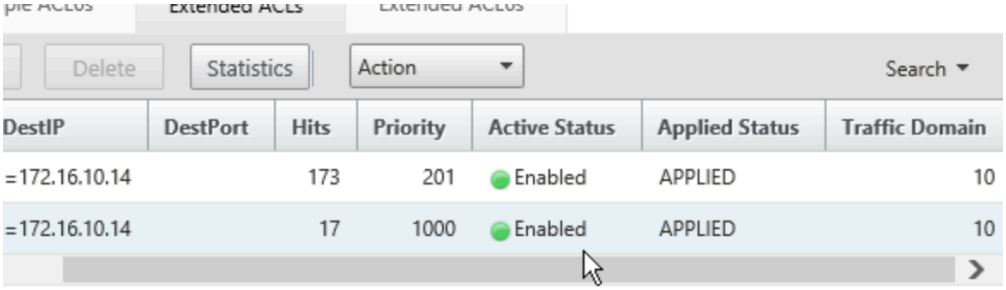
"Action"を選択し、プルダウンから"Apply"を押下します。



確認のホップアップが出ますので[Yes]を選択ください。

アクセス制限の確認 1

画面を右に移動し、"Applied Status"がAPPLIEDになっていることを確認します。



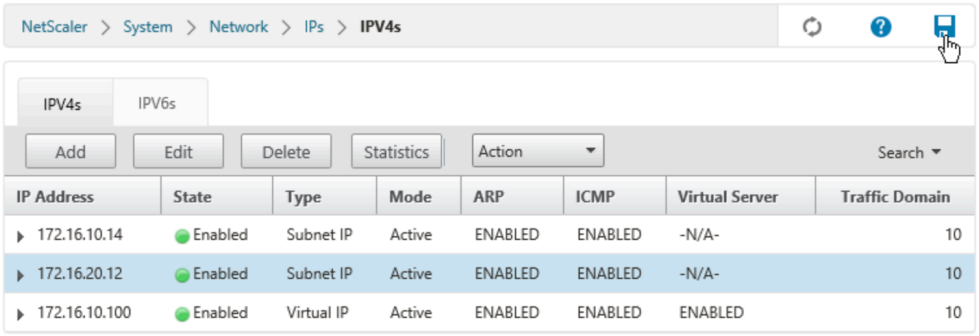
アクセス制限の確認 2

アクセス制限を行ったSNIPに対し、NetScalerの外部からssh、gui(http、https)でのログイン、snmpでの値取得を試み指定した通信のみ可能であることをご確認ください。

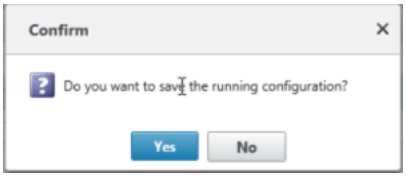
お客様の環境に依存するため、例は載せておりません。

設定の保存

画面右上にフロッピーディスクのマークを押下します。



確認のホップアップが出ますので[Yes]を選択ください。



> ⚠ 本操作を実施しない場合、何らかの理由でNetScalerが再起動した際に変更した設定が全て元の状態に戻ります。
> 必ず設定を保存するようご注意ください。

CLIでの設定方法

以下操作は、NetScalerに対しsshでログインした場合の設定方法を記載します。

ACL設定の確認

```
show ns acl
```

を実行し、既存のACL設定を確認します。

以下の例では、既存のACL設定がないことがわかります。

以降はACLが存在しない前提で設定変更を進めます。

```
> show ns acl
 Done
```

ACL設定

お客様の設計に合わせ以下のようなコマンドで許可する通信、許可しない通信を設定ください。

ログを取得したい場合にはlogstateオプションの利用をご検討ください。

```
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
```

ACL機能に詳細につきましてはCitrix社の公式ドキュメントをご参照ください。

- 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

以下の例では管理用通信が可能なSNIP（172.16.10.14）に対して、192.168.10.100からの通信のみ許可していることがわかります。

```
> 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
```

⚠ アクセスコントロールリスト、ポリシーベースルーティングのPriorityは200番台から利用できます。（1~199は管理用として使用しているため利用できません。）

参考：サービス説明書 制約事項

https://ecl.ntt.com/documents/service-descriptions/loadbalancer/loadbalancer.html#id30

ACL設定の確認

```
show ns acl
```

を実行し、意図したACL設定が適用前の状態(NOTAPPLIED)で入っていることを確認します。

以下の例では設定した2つのACLでApplied StatusがNOTAPPLIEDであることがわかります。

```
> 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
```

ACL設定の適用

```
> apply ns acls
```

を実行し、ACL設定を適用します。

以下の例では、適用処理が完了したことがわかります。

```
> apply ns acls
 Done
```

アクセス制限の確認 1

```
> show ns acl
```

を実行し、ACL設定を確認します。

以下の例では設定したACLが存在し、設定が適用完了（APPLIED）されたことがわかります。

```
> 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
```

アクセス制限の確認２

アクセス制限を行ったSNIPに対し、NetScalerの外部からssh、gui(http、https)でのログイン、snmpでの値取得を試み指定した通信のみ可能であることをご確認ください。

お客様の環境に依存するため、例は載せておりません。

設定の保存

```
save ns config
```

を実行し、変更した設定を保存下さい。

> ⚠ 本操作を実施しない場合、何らかの理由でNetScalerが再起動した際に変更した設定が全て元の状態に戻ります。
>
> 必ず設定を保存するようご注意ください。

改訂履歴

日付	版数	変更点
2017/9/27	1.0.0	初版