

ロードバランサー

Netwiser

SX-3990

SX-3950

SX-3945

SX-3940

SX-3920



第7版

2023年3月28日

U00141575506

セイコーソリューションズ株式会社

© 2018 セイコーソリューションズ株式会社

セイコーソリューションズ株式会社の文書による許可なく、本書の全部または一部の複製、転載および改変などを行うことはできません。

本書の内容については将来予告なしに変更することがあります。

本書に記載された製品（ソフトウェアを含む）の使用に起因する損失、逸失利益などの請求につきましては、いかなる責任も負いかねます。

本書に記載された製品（ソフトウェアを含む）は、日本国内仕様であり、外国の規格などには準拠していません。外国において使用された場合、いかなる責任も負いかねます。

本書に従い、正しい取り扱いをしてください。

はじめに

このたびは Netwiser SX-3920/SX-3940/SX-3945/SX-3950/SX-3990 ロードバランサー(以後、本製品と呼びます)をお買い上げ頂き、まことにありがとうございます。

本書は Netwiser SX-3920/SX-3940/SX-3945/SX-3950/SX-3990 ファームウェアバージョン 8 共通のコマンドリファレンスです。コマンドの機能やフォーマット、パラメーターの意味、使用例、実行例、解説、注意点などを説明しています。

本製品のイーサネットポート数は、お使いになられている製品 (SX-3990 の場合は割り当てた仮想 NIC の数) によって異なります。本書の例では 1-6 などと説明している箇所がありますが、使用されている製品に合わせてお読み替えください。

本製品の関連文書には「**SX-3990_3950_3945_3940_3920 導入・運用の手引**」、「**SX-3950 取扱説明書**」、「**SX-3945,40 取扱説明書**」、「**SX-3920 取扱説明書**」、「**SX-3990 インストールガイド**」があります。

本書で説明している一部のコマンドに関して、製品によりサポート外のコマンドが存在します。「**SX-3990_3950_3945_3940_3920 導入・運用の手引**」と併せてご確認ください。

目次

コマンドリファレンスの書式	1
command	1
グローバルモード	2
config	2
exit	3
export access-log	4
export all	5
export config	6
export licenseid	7
export log	8
export mib	9
export ssl	10
export tech-support	11
export webconf	12
help	13
passwd	14
ping	15
ping6	16
terminal	17
traceroute	18
traceroute6	20
show	22
show コマンド	23
show access-list ipv4	23
show access-list ipv6	24
show access-list mac	25
show access-list mgmt	26
show access-log	27
show advertise-mode	28
show arp	29
show bind	30
show channel	32
show cert-update	34
show cloud-waf	36
show config	37
show connection	38
show content	39

show date.....	40
show environment.....	41
show ethernet.....	42
show history.....	44
show l7-session.....	45
show logging.....	47
show login-session.....	48
show mac.....	49
show nat-pool.....	50
show ndp.....	51
show ntp.....	52
show packet-trace-state.....	53
show probe.....	54
show real.....	56
show route.....	58
show running-config.....	60
show session.....	62
show session-sync.....	63
show socket.....	64
show spanning-tree.....	65
show ssl.....	67
show sticky.....	69
show system.....	72
show tech-support.....	74
show traffic.....	75
show version.....	76
show virtual.....	77
show vlan.....	79
show vrrp.....	80
特権モード.....	82
access-list.....	82
advertise-mode.....	83
allow-ping.....	84
arp.....	85
buddy.....	86
cert-update.....	87
clear access-log.....	88
clear arp.....	89
clear config.....	90

clear content	91
clear logging	92
clear login-session	93
clear mac	94
clear packet-trace	95
clear ssl-session	96
clear statistics	97
cloud-waf	99
copy	100
date	101
dns	102
enable cloud-waf	103
enable probe	104
enable real	105
enable reverse-nat	106
enable virtual	107
halt	108
hostname	109
import all	110
import config	111
import content	112
import firmware	113
import licensekey	114
import ssl	115
import webconf	116
interface	117
ipfw-list	118
l2-trace	119
logging	120
mac	121
maxconns	122
name	123
nat-log	124
nat-pool	125
ndp	126
ntp	127
packet-trace	128
probe	130
proxy	131

real	132
reboot	133
reverse-nat.....	134
route	135
rule	136
snmp	138
spanning-tree	140
ssh	141
ssl	142
ssl session-timeout.....	143
ssl3-enable.....	144
sync	145
system.....	146
telnet.....	147
terminal	148
user-mgmt.....	149
virtual.....	150
vrrp force-backup	151
vrrp instance.....	152
web-mgmt.....	153
write erase	154
write memory.....	155
イーサネット設定モード	156
allowed-vlan	156
channel.....	157
filter	158
firewall	159
mirror-port	160
monitor.....	161
native-vlan	162
protected	163
shutdown	164
slb.....	165
spanning-tree	166
speed	167
tagged.....	168
vlan.....	169
チャンネル設定モード	170
allowed-vlan	170

firewall	170
native-vlan	170
protected	170
slb.....	170
spanning-tree	170
tagged.....	170
vlan.....	170
mode.....	171
VLAN 設定モード	172
filter.....	172
firewall	173
ip address.....	174
ip redundant-address	175
ip virtual-address	176
mtu	177
name	178
route-id.....	179
rtadv.....	180
vlan-mac.....	181
vrrp backup-l2forward	182
vrrp vrid	183
NAT プール設定モード	184
ip address.....	184
リバース NAT 設定モード	185
bind.....	185
enable.....	186
ftp-data-port.....	187
route-id.....	188
timeout	189
SSL 設定モード	190
crl.....	190
csr.....	191
VRRP 設定モード	192
delay	192
interval.....	193
ip peer-address	194
preempt.....	195
priority	196
track	197
ヘルスチェック設定モード	198

dns.....	198
enable.....	199
ftp.....	200
http.....	201
imap4.....	202
interval.....	203
manual-failback	204
ntp.....	205
persist.....	206
pop3.....	207
retry.....	208
smtp.....	209
仮想サーバー設定モード.....	210
access-log.....	210
authfail.....	211
backup-policy.....	212
bind.....	213
certheader.....	215
cipher-suite.....	216
enable.....	217
fallback-url.....	218
ftp-data-port.....	219
header.....	220
match.....	221
name.....	223
onearm-gateway-mode.....	224
permit-nat-filter.....	225
predictor.....	226
route-id.....	227
sidheader.....	228
source-nat.....	229
ssl.....	230
sticky.....	231
timeout.....	233
xff-balancing.....	234
IP アクセスリスト設定モード.....	235
deny.....	235
permit.....	237
IPv6 アクセスリスト設定モード.....	238

deny	238
permit	240
MAC アクセスリスト設定モード	241
deny	241
permit	242
IPFW VLAN リスト設定モード	244
deny	244
permit	246
IPFW イーサネットポートリスト設定モード	248
deny	248
permit	250
SSL 証明書自動更新設定モード	252
check-fqdn.....	252
csr.....	253
csr-update.....	254
enable.....	255
get-account	256
get-password	257
get-url	258
init	259
intermediate-cert-num.....	260
key-password.....	261
put-url.....	262
enable.....	262

コマンドリファレンスの書式

本書では各コマンドを分類別、設定モード別に下記の書式で説明します。

command

機能 この欄ではコマンドの機能について説明しています。

フォーマット [no] command param1 <param2> { param3a | param3b } [param4 <param5>]

param1 は入力が必要なパラメーターです

<param2>, <param5>のように<> 括弧は数値や IP アドレスなど可変な項目を表しています

{ } 括弧は必須選択項目を表しています

[] 括弧は省略可能な項目を表しています

各括弧内で | 縦棒で区切られているパラメーターは、どれか一つを選択する必要がありますことを表しています

コマンドの先頭に位置し、省略可能なパラメータである **no** は、設定を削除する場合や無効にする場合、あるいは設定値をデフォルト値に戻す際に使用するパラメータです

no を指定した時の挙動は、導入・運用の手引を確認してください

パラメーター この欄ではパラメーターの種類と機能について説明しています。

使用例 この欄ではコマンドの使用例を示しています。

実行例 この欄ではコマンドの実行例を表示しています。

解説 この欄ではコマンドのオプションの詳細説明や、表示されるメッセージの内容などについて解説しています。

注意 この欄ではコマンド使用上の注意事項について説明しています。

グローバルモード

シリアルコンソールや、telnet、ssh で本機器へログインすると、グローバルモードに移行します。グローバルモードでは特権モードへの移行、機器情報の参照、設定情報のエクスポート等が行えます。また、自アカウントのパスワード変更など、限られた範囲で設定の変更が行えます。グローバルモードで使用可能なコマンドは、config コマンドを除いた全てのコマンドが特権モードでも使用することができます。

config

機能 グローバルモードから特権モードに移行します。

フォーマット config

パラメーター なし

注意 user-mgmt コマンドで **readonly** 権限が付与されているユーザーでは本コマンドを実行することはできません。

exit

機能 各種設定モードから抜けます。

フォーマット exit

パラメーター なし

解説 グローバルモードで本コマンドを実行した場合、本製品からログアウトします。

export access-log

機能 機器に保存されているテキスト形式の cloud-waf のアクセスログを取り出します。

フォーマット export access-log [tftp | zmodem]

パラメーター tftp | zmodem
tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

export all

機能 システムが動作するために必要な全ての設定情報を取り出します。

フォーマット export all [primary | secondary | current] [tftp | zmodem]

パラメーター primary | secondary | current

primary または secondary 起動領域に保存されている全ての設定情報ファイルを取り出します。 **current** を指定すると現在の起動領域からファイルを取り出します。本パラメーターを省略した場合は **current** となります。

tftp | zmodem

tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

解説 現在の起動領域は **show version** コマンドによって確認することができます。

export config

機能 SSL 関連の鍵、証明書、ソーリーコンテンツなどのファイルを除いた テキスト形式の設定情報ファイルを取り出します。

フォーマット `export config [primary | secondary | current] [tftp | zmodem]`

パラメーター `primary | secondary | current`
primary または secondary 起動領域に保存されている設定情報ファイルを取り出します。 **current** を指定すると現在の起動領域からファイルを取り出します。本パラメーターを省略した場合は **current** となります。

tftp | zmodem

tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

解説 現在の起動領域は `show version` コマンドによって確認することができます。

export licenseid

機能 NetwiserVE EP 版のアクティベート用認証 ID を取り出します。

フォーマット export licenseid [tftp | http]

パラメーター tftp | http
tftp または http によって認証 ID を取り出します。省略時は tftp 動作となります。

MEMO このコマンドは非公開コマンドです。

export log

機能 機器に保存されているテキスト形式のログを取り出します。

フォーマット export log [tftp | zmodem]

パラメーター tftp | zmodem

tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

export mib

機能 本機器の SNMP 拡張 MIB ファイルを取り出します。

フォーマット export mib [tftp | zmodem]

パラメーター tftp | zmodem

tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

export ssl

機能 SSL アクセラレーションで使われる秘密鍵や証明書などを取り出します。

フォーマット `export ssl <policy-name> { cert | chain | client | crl | csr | key | pkcs12 } [tftp | zmodem]`

パラメーター `<policy-name>`
特権モードの `ssl` コマンドで作成した SSL ポリシーの名前を指定します。

cert

サーバー証明書を取り出します。

chain

中間 CA 局の証明書を取り出します。証明書がチェーンされている場合にはすべての中間 CA 局証明書が取り出されます。

client

クライアント証明書を署名した認証局の証明書を取り出します。証明書がチェーンされている場合にはすべて取り出されます。

crl

証明書失効リストを取り出します。

csr

証明書署名要求を取り出します。

key

秘密鍵を取り出します。

pkcs12

秘密鍵、証明書、中間証明書をまとめて PKCS#12 形式で取り出します。

tftp | zmodem

tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

解説 取り出した秘密鍵ファイルや PKCS#12 形式のファイルは本機器によって自動的に暗号化されます。

注意 取り出したファイルはウェブサーバー等にインポートすることはできません。

export tech-support

機能 本機器の技術サポートを受ける場合に必要となるファイルを取り出します。

フォーマット `export tech-support { ftp | scp } <host-addr> <path> <usr>`

パラメーター `ftp | scp`

リモートへの転送プロトコルに FTP または SCP を使用します。

`<host-addr>`

転送先の IP アドレスを指定します。

`<path>`

ファイルを格納する宛先のファイルパスを絶対パスで指定します。

`<user>`

宛先のログインアカウント名を指定します。

export webconf

機能 WEB 管理画面の表示/非表示状態を記述したテキスト形式の設定情報ファイルを取り出します。

フォーマット export webconf [tftp | zmodem]

パラメーター tftp | zmodem
tftp または zmodem によってファイルを取り出します。省略時には **tftp** 動作となります。

help

機能 各コマンドの使用方法を表示します。

フォーマット `help <command>`

パラメーター `<command>`
`<command>`コマンドの使用方法を表示します。

実行例

```
netwiser> help ping
Commands available:
ping {<ipv4-addr> | <host-name>}
```

```
netwiser> help ping6
Commands available:
ping6 {<ipv6-addr> | <host-name>}
```

passwd

機能 現在ログインしているユーザーのパスワードを変更します。

フォーマット passwd

パラメーター なし

解説 変更したパスワードは CLI でのログインと、WebUI でのログインの両方に適用されます。

ping

機能 ICMP echo によってホストへの到達性を確認します。

フォーマット `ping { <ipv4-addr> | <host-name> }`

パラメーター <ipv4-addr>
宛先ホストの IPv4 アドレス

<host-name>
宛先ホストのホスト名。DNS サーバーが設定されている場合にのみ使用することができます。

ping6

機能 ICMPv6 echo によってホストへの到達性を確認します。

フォーマット `ping6 { <ipv6-addr> | <host-name> }`

パラメーター <ipv6-addr>
宛先ホストの IPv6 アドレス

<host-name>
宛先ホストのホスト名。DNS サーバーが設定されている場合にのみ使用することができます。

terminal

機能 コマンドライン表示のページングを設定します。

フォーマット [no] terminal pager [more]

パラメーター なし

解説 `no terminal pager more` を実行するとページングを停止します。デフォルトの動作ではページングを行います。`more` キーワードは省略可能です。

traceroute

機能 宛先ホストまでのネットワーク経路をリスト表示します。

フォーマット `traceroute { <ipv4-addr> | <host-name> } [source-ip-addr <ipv4-addr> [route-id <num>] | source-virtual {<virtual-id> | <virtual-name>}] [hop <num>]`

パラメーター `<ipv4-addr>`

宛先ホストの IPv4 アドレス

`<host-name>`

宛先ホストのホスト名。

DNS サーバーが設定されている場合にのみホスト名を指定することができます。

source-ip-addr

送信元 IP アドレスを指定します。

`<ipv4-addr>`

送信元の IPv4 アドレス

route-id

使用するルーティングテーブルのルート ID を指定します。

`<num>`

ルート ID

入力値範囲:0 から 15

source-virtual

送信元の仮想サーバーID または仮想サーバー名を指定します。

`<virtual-id>`

送信元の仮想サーバーID

`<virtual-name>`

送信元の仮想サーバー名

hop

最大ホップ数を指定します。

省略した場合、8 に設定されます。

`<num>`

ホップ数

入力値範囲:1 から 32

traceroute6

機能 宛先ホストまでのネットワーク経路をリスト表示します。

フォーマット `traceroute6 { <ipv6-addr> | <host-name> } [source-ip-addr <ipv6-addr> [route-id <num>] | source-virtual { <virtual-id> | <virtual-name> }] [hop <num>]`

パラメーター <ipv6-addr>

宛先ホストの IPv6 アドレス

<host-name>

宛先ホストのホスト名。

DNS サーバーが設定されている場合にのみホスト名を指定することができます。

source-ip-addr

送信元 IP アドレスを指定します。

<ipv6-addr>

送信元の IPv6 アドレス

route-id

使用するルーティングテーブルのルート ID を指定します。

<num>

ルート ID

入力値範囲:0 から 15

source-virtual

送信元の仮想サーバーID または仮想サーバー名を指定します。

<virtual-id>

送信元の仮想サーバーID

<virtual-name>

送信元の仮想サーバー名

hop

最大ホップ数を指定します。

省略した場合、8 に設定されます。

<num>

ホップ数

入力値範囲:1 から 32

show

機能 各種情報を表示します。

フォーマット `show <param1> [<param2> ...]`

パラメーター パラメーターについては各 show コマンドの説明をご参照ください。

show コマンド

機器情報の参照に使用するコマンドを説明します。show コマンドはグローバルモードを含むすべての設定モードで使用することができます。

show access-list ipv4

機能 機器に適用されている IPv4 アクセスリストの一覧を表示します。

フォーマット show access-list ipv4

パラメーター なし

実行例

```
line    matches action
=====
vlan3:
  10      1598 permit tcp 10.0.73.170 10.208.12.171 eq http
  11      134 permit tcp 10.0.20.82 10.208.12.171
  12       75 permit tcp 10.0.20.83 10.208.12.171
  13      33 permit tcp 10.0.21.15 10.208.12.171
  14       0 permit tcp 10.0.75.31 10.208.12.171
  15      77 permit tcp 10.0.75.12 10.208.12.171
  20     3735 deny ip any 10.0.12.171 log
  30    331507 permit ip any any
65535      0 deny ip any any

vlan4094:
65535    432340 deny ip any any
```

解説 line
設定したアクセスリストの行番号が表示されます。行番号の若いフィルターリングエントリーから評価されます。

matches
アクセスリストにマッチしたパケットの数が表示されます。

action
パケットに対する動作(許可、拒否)とマッチするパケットの内容が表示されません。

show access-list ipv6

機能 機器に適用されている IPv6 アクセスリストの一覧を表示します。

フォーマット show access-list ipv6

パラメーター なし

実行例

```
line matches action
=====
vlan10:
 1    42523 permit tcp 2001:db8::/96 eq https
 2    890310 permit tcp 2001:db8::20:82 2001:db8::12:171
 3    10023 permit tcp 2001:db8::20:83 2001:db8::12:171
 4     394 permit tcp 2001:db8::21:15 2001:db8::12:171
10   55820349 deny ip any any
```

解説 **line**
設定したアクセスリストの行番号が表示されます。行番号の若いフィルターリングエントリーから評価されます。

matches
アクセスリストにマッチしたパケットの数が表示されます。

action
パケットに対する動作(許可、拒否)とマッチするパケットの内容が表示されます。

show access-list mac

機能 機器に適用されている MAC アクセスリストの一覧を表示します。

フォーマット show access-list mac

パラメーター なし

実行例

```
line    matches action
=====
port6: inbound
  10      262 permit 00:80:15:1f:03:6e any
  20      17  permit 00:80:15:1f:03:7e any
65535    2471 deny any any
-----
port6: outbound
  10      915 permit any 00:80:15:1f:03:8e
  20      911 permit any 00:80:15:1f:03:9e
65535    1007 deny any any
=====
```

解説 **line**
設定したアクセスリストの行番号が表示されます。行番号の若いフィルターリングエントリから評価されます。

matches
アクセスリストにマッチしたパケットの数が表示されます。

action
パケットに対する動作(許可、拒否)とマッチするパケットのアドレスが表示されます。

portN
アクセスフィルターが適用されているイーサネットポートを示しています。

inbound / outbound
それぞれ受信パケット、送信パケットに対して適用されるアクセスリストであることを示しています。

show access-list mgmt

機能 機器に適用されている管理アクセスリストを表示します。

フォーマット show access-list mgmt

パラメーター なし

実行例

```
matches action
=====
ip:
  923301 permit tcp 0.0.0.0/0 any eq ssh
    0 deny tcp any any eq ssh
  183 deny tcp any any eq telnet
  78 permit tcp 0.0.0.0/0 any eq http
  2240 permit tcp 0.0.0.0/0 any eq https
    0 deny tcp any any eq http
    0 deny tcp any any eq https
  15 deny udp any any eq snmp

ipv6:
  0 permit tcp ::/0 any eq ssh
  0 deny tcp any any eq ssh
  0 deny tcp any any eq telnet
  0 permit tcp ::/0 any eq http
  0 permit tcp ::/0 any eq https
  0 deny tcp any any eq http
  0 deny tcp any any eq https
  0 deny udp any any eq snmp
```

解説 本コマンドの表示は、特権モードの **telnet**, **ssh**, **web-mgmt**, **snmp** コマンドに連動して変化します。

matches

アクセスリストにマッチしたパケットの数が表示されます。

action

パケットに対する動作(許可、拒否)とマッチするパケットの内容が表示されます。

show access-log

機能 cloud-waf のアクセスログを表示します。

フォーマット show access-log

パラメーター なし

実行例

```
163.49.52.30 -- [17/Mar/2023:11:08:46 +0900] "GET
/WebGoat/images/buttons/lessonComplete.jpg HTTP/1.1" 200 613
163.49.52.30 -- [17/Mar/2023:11:08:46 +0900] "GET /WEB-
INF%2Fweb.xml/images/buttons/javaOver.jpg HTTP/1.1" 404 241
163.49.52.30 -- [17/Mar/2023:11:08:46 +0900] "GET
/WebGoat/images/buttons/lessonComplete.jpg HTTP/1.1" 200 613
```

show advertise-mode

機能 GARP、UNA の送信状態を表示します。

フォーマット show advertise-mode

パラメーター なし

実行例

advertise-mode on の場合 (GARP、UNA 送信中)
Now running... (590 seconds remaining)

advertise-mode off の場合 (GARP、UNA 送信停止中)
Stopped now.

解説 GARP、UNA 送信中は送信の残り時間を表示します。

show arp

機能 ARP キャッシュを表示します。

フォーマット show arp

パラメーター なし

実行例

IP Address	MAC Address	Interface	Expire	Flags
10.0.10.1	c0:8c:60:54:6a:6e	vlan999	1189	
10.0.10.70	00:80:15:d1:00:1e	vlan999		
10.0.10.71	00:80:15:d1:00:1e	vlan999		pns
192.168.0.1	00:80:15:d1:00:1e	vlan1		

解説 IP Address
ホストの IP アドレスが表示されます。

MAC Address
ホストの MAC アドレスが表示されます。

Interface
ホストが存在する VLAN インターフェイスが表示されます。

Expire
ARP キャッシュが失効するまでの残り時間が表示されます。空欄の場合は permanent エントリーであることを示しています。

Flags
エントリーの動作状態が表示されます。p=published, n=network, s=server, t=transparent を意味します。エントリーが仮想 IP アドレスのものであれば有効/無効に連動して p フラグが変化します。透過モード動作のときは t フラグが ON となります。透過モード動作では仮想 IP アドレスが有効のときには p は ON にならず実サーバーがヘルスチェックによって DOWN と判定されたときのみ p が ON となります。n と s は network ポート、server ポートからの ARP 要求に回答することを意味し、透過モードのときは s が OFF のとなります。

show bind

機能 仮想サーバーと、仮想サーバーにバインドされた実サーバーの接続情報を表示します。

フォーマット show bind [<virtual-id>]
ト

パラメータ <virtual-id>
— 表示させたい仮想サーバーID、または仮想サーバー名を指定します。省略された場合、全仮想サーバーについて表示します。

実行例

Server-Id	Curr (R)	Peak (R)	Total (R)	Curr (B)	Peak (B)	Total (B)	Max	Enable
V1. 80. tcp	0	45487	2810126781	-	-	-		yes
S1. 80 [1]	0	70	41841720	0	0	0	3000	yes
S4. 80 [1]	0	126	1295150652	0	0	0	100	yes
S5. 80 [1]	0	0	0	0	0	0	0	yes
S2. 80 [2]	0	38585	2289898513	0	38585	2248067321	0	yes
S3. 80 [3]	0	12047	593173682	0	12047	562059460	0	yes

解説 Server-Id
一番上に仮想サーバーIDが表示されます。半角スペースで1段下がっているエントリは実サーバーIDを示しています。[]括弧内にはbindで指定したグループ番号が表示されます。

Curr(R)
現在接続中の接続数が表示されます。
実サーバーID単位(システム全体)の接続数です。

Peak(R)
接続数のピーク値が表示されます。
実サーバーID単位(システム全体)のピーク値です。

Total(R)
現在までに処理した接続の累積カウントが表示されます。
実サーバーID単位(システム全体)の累積カウントです。

Curr(B)
現在接続中の接続数が表示されます。
仮想サーバーID単位(仮想サーバー毎)の接続数です。

Peak(B)
接続数のピーク値が表示されます。

仮想サーバーID 単位(仮想サーバー毎)のピーク値です。

Total(B)

現在までに処理した接続の累積カウントが表示されます。

仮想サーバーID 単位(仮想サーバー毎)の累積カウントです。

Max

maxconns コマンドで設定された最大接続数が表示されます。仮想サーバーには **maxconns** コマンドが適用されませんので空欄となります。

Enable

各仮想サーバーID、実サーバーID が **enable** に設定されていると **yes** が表示されます。

実サーバーID 単位の数値は、該当の実サーバーID がバインドされた全ての仮想サーバーの合算値を示しています。

仮想サーバーID 単位の数値は、該当の実サーバーID の仮想サーバー毎の値を示しています。

show channel

機能 論理チャネルの状態を表示します。

フォーマット show channel

パラメーター なし

実行例

```
Group          State Ports
1              up    1 2
```

```
Port  Flags  Actor ID          State  Partner ID          State
1     ACDE   8000.00:80:15:d1:04:6c 3d    8000.4c:00:82:4b:1d:80 3d
2     ACDE   8000.00:80:15:d1:04:6c 3d    8000.4c:00:82:4b:1d:80 3d
```

解説 論理チャネル毎に下記の情報が表示されます。

Group

論理チャネル番号が表示されます。

State

論理チャネルの状態で up/ down が表示されます。

Ports

この論理チャネルに所属するイーサネットポート番号が表示されます。

イーサネットポート毎に下記の情報が表示されます。

Port

集約されているイーサネットポート毎の情報が表示されます。

Flags

集約ポートの動作状態が表示されます。

各フラグはそれぞれ以下の状態を表します。

A : port is active

C : port is receiving frames

D : port is sending frames

E : port is enabled

Actor / Partner ID

lacp モードのときに使用される ID を示します。Actor と Partner はそれぞれ本製品、対向機を意味します。

State

LACPDU で交換されている LACP の状態を示します。

show cert-update

機能 証明書自動更新情報を表示します。

フォーマット show cert-update [*prefix*]
ト

パラメータ prefix

- 指定した証明書自動更新情報を表示します。本パラメーターを省略した場合は全て表示となります。

実行例

```
cert-update cud_ssl
Processing ssl: cud_ssl_1    status: Wait for certificate
      CSR: eeed0be4ee07927b8cb5b837b6bba2a0
      Make ssl: 0    Make csr: 0
      Upload csr: 1    Upload err: 0
      Download cert: 69    Download err: 0
      Bad cert: 69    Bad key: 0
      Cert updated: 0    Effect to virtual: 0
      Next interval: 16:11:00
```

解説 Processing ssl
更新対象または更新中の SSL ポリシー名です。
Status
更新状況です。
-- : 状態確認中、または CSR なしモード
Idle : 現証明書は有効期間中
Process CSR : 有効期間が設定した期日になったため、SCR を作成し、サーバーへアップロード準備中
Wait for certificate : CSR アップロードが完了し、証明書のダウンロード待ち
Check cert : ダウンロードした証明書を確認中
CSR
作成した CSR の同一性を確認するための、MD5 のハッシュ値

以下は証明書自動更新の統計情報です。
Make ssl
新しく証明書(と鍵)をダウンロードするために SSL ポリシーを作成した回数
Make csr
CSR を作成した回数
Upload csr
CSR をアップロードした回数
Upload err

CSR アップロードが失敗した回数

Download cert

証明書(と鍵)をダウンロードした回数

Download err

証明書(と鍵)のダウンロードが失敗した回数

Bad cert

ダウンロードした証明書のフォーマット異常、期限切れ、鍵との不整合

Bad key

ダウンロードした鍵のフォーマット異常

Cert updated

ダウンロードが正常に終了した回数

Effect to virtual

新しい SSL ポリシーが仮想サーバーへ更新された回数

※仮想サーバーへの更新は毎日 15:00~16:59 の間となります。

Next interval

証明書自動更新は 1 時間のインターバルで段階的に処理が進みます。

その時刻が表示されます。

show cloud-waf

機能 クラウド WAF の設定情報を表示します。

フォーマット show cloud-waf [-d]

パラメーター -d
Block IP List を表示します。

実行例 デフォルト表示 (-d オプションなし)

```
Manager-Address: 3.114.226.161
Port: 10024
Key: ID: 002, Name: SVB000000024, IP: any
Enable: yes
```

-d オプション指定時

```
Manager-Address: 3.114.226.161
Port: 10024
Key: ID: 002, Name: SVB000000024, IP: any
Enable: yes
```

```
--- Block IP List ---
163.49.52.30/32
```

解説

Manager-Address
クラウド WAF マネージャーの IP アドレスが表示されます。

Port
クラウド WAF マネージャーの宛先ポート番号が表示されます。

Key
クラウド WAF マネージャーより発行されたエージェントキーの内容が表示されます。

Enable
クラウド WAF の設定状態です。有効の場合 yes と表示されます。

Block IP List
ブロックされている IP アドレスが表示されます。

show config

機能 フラッシュメモリーに保存されている設定情報を表示します。

フォーマット show config [primary | secondary | current]

パラメーター primary | secondary | current

primary または secondary 起動領域に保存されている設定情報を表示します。
current を指定すると現在の起動に保存されている設定を表示します。本パラメーターを省略した場合は **current** となります。

解説 現在の起動領域は **show version** コマンドによって確認することができます。

show connection

機能 負荷分散に関連するセッション情報の現在値とピーク値を表示します。

フォーマット show connection

パラメーター なし

実行例

Type	Current	Peak
====	=====	=====
L4 Sessions	29856	32905
IP Sticky	257628	725790
Cookie Sticky	193	99823
FTP Proxy	0	10
APP Proxy	1673	33256
SSL Proxy	321	23456

解説 L4 Sessions
L4 負荷分散で処理されているセッション情報数が表示されます。

IP Sticky
IP セッション維持情報の数が表示されます。

Cookie Sticky
COOKIE セッション維持情報の数が表示されます。insert モードのときはこのカウントが増えることはありません。

FTP Proxy
FTP 負荷分散のセッション情報数が表示されます。

APP Proxy
L7 負荷分散のセッション情報数が表示されます。IPv4→IPv6、IPv6→IPv4 変換をしている場合にもこのカウントが増えます。

SSL Proxy
SSL アクセラレータのセッション情報数が表示されます。

show content

機能 システムにインポートしたソーリーコンテンツを表示します。

フォーマット `show content <content-name>`

パラメーター なし

実行例

```
netwiser$ show content sorry_html
```

```
<!DOCTYPE html>
<html lang="ja">
  <head>
    <meta charset="utf-8">
  </head>
  <body>
    ただいまサーバーが混雑しています。しばらく経ってから再度接続してください。
  </body>
</html>
```

注意 インポートしたファイルがそのまま表示されますので、文字コードによっては文字化けして表示される場合があります。

show date

機能 現在の時刻を表示します。

フォーマット show date

パラメーター なし

実行例

Thu Sep 15 00:39:50 JST 2018

show environment

機能 CPU 使用率、メモリー使用率、CPU 温度のリアルタイム統計情報を表示します。

フォーマット show environment

パラメーター なし

実行例

```
CPU          : 9 %
MEMORY       : 5 %
TEMPERATURE  : 43.0 deg C
PSU_A        : GOOD
PSU_B        : NOT_PRESENT
```

解説

CPU:
CPU 使用率が表示されます。

MEMORY:
メモリー使用率が表示されます。

TEMPERATURE:
CPU 温度が表示されます。

PSU_A:
PSU_B:
冗長電源の状態が表示されます。本項目が表示されるのは SX-3950 のみです。

GOOD:
電源良好

FAULT:
電源 OFF または電源故障

NOT_PRESENT:
電源未挿入

FAN_FAULT:
ファン故障

show ethernet

機能 イーサネットポートの送受信パケット数の累積値を表示します。

フォーマット `show ethernet [<port-num>]`

パラメーター `<port-num>`

本機器の技術サポートのために使用されるオプションです。指定された物理インターフェイスの詳細情報を表示します。

実行例 1 フェイルスルーをサポートしていない製品の表示

Port	Address	Speed	State	RxPkts	TxPkts	RxErrs	TxErrs
1	00:80:15:d1:02:3a	1000F	up	7606	55288	0	0
2	00:80:15:d1:02:3a	1000F	up	22375	68781	0	0
3	00:80:15:d1:02:3a	1000F	up	93536	63051	0	0
4	00:80:15:d1:02:3d	100H	down	0	0	0	0
5	00:80:15:d1:02:3e	100H	down	0	0	0	0
6	00:80:15:d1:02:3f	100H	down	0	0	0	0
7	00:80:15:d1:02:40	100H	down	0	0	0	0
8	00:80:15:d1:02:41	1000H	down	0	93930	0	0
9	00:80:15:d1:02:42	1000F	up	158094	7953	0	0
10	00:80:15:d1:02:43	1000F	up	588	594	0	0

実行例 2 フェイルスルーをサポートしている製品の表示

Port	Address	Speed	State	RxPkts	TxPkts	RxErrs	TxErrs
1	00:80:15:d1:06:0c	1000F	up	1672296	1338271	0	0
2	00:80:15:d1:06:0d	1000F	up	13983	20865	0	0
3	00:80:15:d1:06:0e	1000F	up	1200213	1205578	0	0
4	00:80:15:d1:06:0f	1000F	up	486027	494615	0	0
5	00:80:15:d1:06:10	1000F	up	95868	337692	0	0
6	00:80:15:d1:06:11	1000F	up	0	6431848	0	0

Relay: on

Through Switch: on

解説 Port
イーサネットポートの番号を示しています。

Address
イーサネットポートが使用している MAC アドレスが表示されます。

Speed
リンク速度と duplex が表示されます。数字はリンク速度、F/H はそれぞれ全二重と半二重を意味します。

State

リンク状態が up または down で表示されます。

RxPkts / TxPkts

受信パケット数、送信パケット数が表示されます。

RxErrs / TxErrs

受信エラー数、送信エラー数が表示されます。

Relay

スルーポートが正常に機能している場合 on、障害が検知されている場合は off が表示されます。

Through Switch

スルー機能が物理的に有効になっている場合 on、無効になっている場合は off が表示されます。

show history

機能 実行したコマンドの履歴を表示します。

フォーマット show history [all]

パラメーター all

CLI と WebUI で実行したコマンドの履歴全てを表示します。このパラメーターを省略した場合は、現在のログインセッションで実行したコマンドの履歴が表示されます。

実行例

```
1 show forward
2 show history
3 show running-config interface vlan
4 ping 10.208.10.1
5 show history
6 show config
7 show version primary
8 show version secondary
9 show history
```

show l7-session

機能 現在処理中の L7 負荷分散セッション情報を表示します。

フォーマット `show l7-session [<ip-addr> | <ip-addr,port>] [-d]`

パラメーター <ip-addr>, <ip-addr,port>

表示させたい IP アドレスを指定します。数値をドット(.)で繋げてポート番号を含めて指定することも可能です。

省略された場合、全 L7 セッションについて表示します。

-d

より詳細な情報を表示します。

クライアント側セッション情報、サーバー側セッション情報の順に 2 行 1 組で表示されます。

実行例 デフォルト表示 (-d オプションなし)

Proto	Client	Virtual	Real
tcp	10.208.11.100.51460	10.208.10.95.80	10.208.11.101.80
tcp	10.208.11.100.51458	10.208.10.95.80	10.208.11.101.80
tcp	10.208.11.100.51459	10.208.10.95.80	10.208.11.101.80

-d オプション指定時

P	Recv-Q	Send-Q	Local Address	Foreign Address	State
t	0	0	10.208.10.95.80	10.208.11.100.54202	IDLE
	0	0	-----	-----	INIT
t	0	0	10.208.10.95.80	10.208.11.100.54200	CLOSING
	0	0	10.208.10.95.42904	10.208.11.101.80	WAIT_CLOSE
t	137	0	10.208.10.95.80	10.208.11.100.54201	IDLE
	0	0	10.208.10.95.60434	10.208.11.101.80	CONNECTING

解説 Proto
tcp または udp でプロトコルを表します。

Client
クライアント IP アドレスと送信元ポートを表示します。

Virtual
仮想サーバー IP アドレスと待ち受けポートを表示します。

Real
実サーバー IP アドレスと待ち受けポートを表示します。

P

-d オプション指定時にはこの列でプロトコルを表示します。
tcp であれば't'、udp であれば'u'が表示されます。ただし、表示されるのはクライアント側セッションのみです。

Recv-Q / Send-Q

送受信待ちのデータサイズが表示されます。

Local Address

本機器側の IP アドレスとポート番号が表示されます。
クライアント側/サーバー側どちらか一方のセッションのみが存在している場合、もう片方のセッションには連続したハイフン(-)のみが表示されます。

Foreign Address

相手側の IP アドレスとポート番号が表示されます。
クライアント側/サーバー側どちらか一方のセッションのみが存在している場合、もう片方のセッションには連続したハイフン(-)のみが表示されます。

State

L7 セッションの接続状態が表示されます。

show logging

機能 機器のシステムログを表示します。

フォーマット `show logging`

パラメーター なし

実行例

```
Aug 26 09:40:52 netwiser lbhcd: health check daemon start
Aug 26 09:40:51 netwiser lbsyncd: state changed to backup
Aug 26 09:40:51 netwiser lbstatd: statistics daemon start
Aug 26 09:40:51 netwiser lbvrrpd: (backup) delay=0
```

show login-session

機能 現在のログインユーザーの一覧を表示します。

フォーマット show login-session

パラメーター なし

実行例

Term-ID	User	Term-Name	Permission	Host
0*	manager	ttyu0	Admin	localhost, 1519
1	operator	pts/0	ReadOnly	10.208.10.19, 7072

解説 Term-ID
システムが端末毎に割り当てる ID が表示されます。
特権モード以降の設定モードに遷移しているユーザーの端末 ID 末尾には、*が
付加されます。

User
ログイン中のユーザーのユーザー名が表示されます。

Term-Name
端末名が表示されます。

Permission
ログインユーザーの権限が Admin または ReadOnly で表示されます。

Host
ログイン元の IP アドレスと実行プロセスの PID が表示されます。

show mac

機能 MAC アドレステーブルを表示します。

フォーマット show mac

パラメーター なし

実行例

VLAN	MAC Address	Interface	Expire
100	00:80:15:d1:01:b0	port1	1199
200	00:80:15:d1:01:b0	chan1	1185
1300	00:00:5e:00:02:6f	port9	1200
1300	00:00:5e:00:01:6f	port9	1200
1300	00:00:5e:00:01:6e	port9	1200
1300	00:00:5e:00:02:8d	port9	1200

解説 VLAN
MAC アドレスが存在する VLAN の VLAN ID が表示されます。表示は VLAN ID でソートされます。

MAC Address
MAC アドレスが表示されます。

Interface
MAC アドレスが存在するイーサネットポートまたは論理チャネル名が表示されます。

Expire
エントリーが失効するまでの残り時間が秒単位で表示されます。

show nat-pool

機能 NAT プールの統計情報を表示します。

フォーマット show nat-pool

パラメーター なし

実行例

```
ipv4:
Proto Address          Refs InUse  Requests    Full
tcp   10.0.0.144          1    0    267         0
tcp   10.0.0.143          1 2239 5576066    3696280
```

```
ipv6:
Proto Address          Refs InUse  Requests    Full
tcp   fd00::144          1    0    23567       0
tcp   fd00::143          1 5235 4217792    3990845
```

解説 IPv4 と IPv6 アドレス毎に統計情報が表示されます。

Proto

プールアドレスが使用しているプロトコルを表示されます。tcp または udp が表示されます。同じ IP アドレスに対して tcp と udp が両方表示される場合もあります。

Address

プールアドレスが表示されます。

Refs

このアドレスを使用しているソース NAT やリバース NAT の個数が表示されません。

InUse

このアドレスを使用している接続の現在の数が表示されます。

Requests

このアドレスに対して空きポートの検索を試行した数が表示されます。

Full

このアドレスで使用できるポートを使い切った状態で Requests した数が表示されます。

show ndp

機能 IPv6 近隣キャッシュを表示します。

フォーマット show ndp

パラメーター なし

実行例

IPv6 Address Flags	MAC Address	Interface	Expire	State
fe80::280:15ff:fed1:1e able	00:80:15:d1:00:1e	vlan3	permanent	reach
fd00::10:70 able	00:80:15:d1:00:1e	vlan999	permanent	reach
fd00::10:71 able pns	00:80:15:d1:00:1e	vlan999	permanent	reach
fe80::280:15ff:fed1:1e able	00:80:15:d1:00:1e	vlan999	permanent	reach
fd00::11:100 able	00:0c:29:77:91:30	vlan999	14s	reach
fe80::20c:29ff:fe77:9130 fe80::280:15ff:fed1:1e able	00:0c:29:77:91:30 00:80:15:d1:00:1e	vlan999 vlan1	4s permanent	delay reach

解説 IP Address
ホストの IPv6 アドレスが表示されます。

MAC Address
ホストの MAC アドレスが表示されます。

Interface
ホストが存在する VLAN インターフェイスが表示されます。

Expire
後述の State 状態が失効するまでの残り時間が表示されます。

State
RFC 2461 で規定された近隣キャッシュの状態が表示されます。

Flags
Flags の意味については **show arp** コマンドの Flags の項目をご参照ください。

show ntp

機能 NTP サーバーとの同期状態を表示します。

フォーマット show ntp

パラメーター なし

実行例

```
remote          refid          st t when poll reach  delay  offset  jitter
=====
*10.208.11.158  10.208.9.89    2 u 111 256 377  0.227  0.179  0.508
```

解説 remote
NTP サーバーの IP アドレスが表示されます。同期している場合 IP アドレスの左に*マークが表示されます。

refid
NTP サーバーが同期している同期先が表示されます。

st
サーバーの NTP 階層が表示されます。

show packet-trace-state

機能 パケットトレース機能の情報を表示します。

フォーマット show packet-trace-state

パラメーター なし

実行例

```
trace-mode          : L7
packet-trace(state) : on
packet-trace(config) : on
```

```
filter(ipv4) :
```

```
filter(ipv6) :
permit ip fd00::11:100 port 8080 and-policy
```

```
Total capture size : 0
```

解説 trace-mode
動作しているトレース機能の種別(L2/L7)を表示します。
トレース機能が on の場合のみ表示されます。

packet-trace(state)
トレース機能の on/off 状態を表示します。実際の動作状態を表し、設定状態と異なる場合もあります。

packet-trace(config)
トレース機能の設定上の on/off 状態を表示します。
トレース機能が自動停止した場合でも、**packet-trace off** コマンドが実行されない限り本項目が off になることはありません。

filter(ipv4), filter(ipv6)
設定中のフィルター情報を表示します。
動作しているトレース機能が L2 の場合、filter(ipv6)は表示されません。

Total capture size
現在までに内部 disk に保存したキャプチャサイズの総計を表示します。
packet-trace off またはシステムによる自動停止のタイミングで更新されません。

show probe

機能 サーバーヘルスチェックの状態を表示します。

フォーマット `show probe [<probe-name>] [-r | -d]`

パラメーター <probe-name>

表示させたいヘルスチェックポリシー名を指定します。
省略された場合、全ヘルスチェックポリシーについて表示します。

-r

ヘルスチェック情報を一行で表示させるためのオプションです。デフォルト表示と異なり、ヘルスチェック情報を一行毎に表示します。

-d

ヘルスチェック情報を一行で表示させるためのオプションです。**-r**に加え、より詳細な情報を表示します。

実行例 デフォルト表示 (**-r, -d** オプションなし)

```
Name: www-sv1          Server: 10.6.201.5
                        Port: 80      Pass: 2014      State: ALIVE
                        Proto: tcp    Fail: 1
                        Enable: yes
```

```
Name: www-sv2          Server: 172.16.22.4
                        Port: 80      Pass: 2014      State: ALIVE
                        Proto: tcp    Fail: 1
                        Enable: yes
```

-r オプション指定時

```
Name          Server          State Enable
www-sv1       10.6.201.5.80.tcp    ALIVE  yes
www-sv2       172.16.22.4.80.tcp  ALIVE  yes
```

-d オプション指定時

```
Name          Server          Pass    Fail
State Enable
www-sv1       10.6.201.5.80.tcp    2014    1 ALI
VE  yes
www-sv2       172.16.22.4.80.tcp  2014    1 ALI
VE  yes
```

解	説	Name	ヘルスチェックのポリシー名が表示されます。
		Server, Port, Proto	ヘルスチェック対象の IP アドレス、ポート番号、プロトコルが表示されます。
		Enable	ヘルスチェックの設定状態です。有効の場合 yes と表示されます。
		Pass / Fail	ヘルスチェックが成功 / 失敗した回数が表示されます。
		State	現在のサーバーの状態が表示されます。ALIVE の場合サーバーは正常です。DOWN になると負荷分散対象から除外されます。

show real

機能 実サーバー毎の統計情報を表示します。

フォーマット `show real [<server-id>] [-r | -d]`

パラメーター `<server-id>`

表示させたい実サーバーIDを指定します。
省略された場合、全実サーバーについて表示します。

-r

実サーバー情報を一行で表示させるためのオプションです。デフォルト表示と異なり、実サーバー情報を一行毎に表示します。

-d

実サーバー情報を一行で表示させるためのオプションです。**-r**に加え、より詳細な情報を表示します。

実行例 デフォルト表示 (**-r, -d** オプションなし)

Address: fd00:709::5

Port: 80	Curcon: 865
Proto: tcp	PeakCon: 3877
MaxCon: 0	TotCon: 156895
Enable: yes	Fail: 0

Address: 2001:380:283:710::4

Port: 69	Curcon: 1
Proto: udp	PeakCon: 2
MaxCon: 0	TotCon: 3
Enable: yes	Fail: 2

Address: 10.6.201.2

Port: 123	Curcon: 2
Proto: udp	PeakCon: 2
MaxCon: 0	TotCon: 2
Enable: yes	Fail: 0

-r オプション指定時

Real	Curcon	TotCon	Fail	Enable
fd00:709::5. 80. tcp	865	3877	0	yes
2001:380:283:710::4. 69. udp	1	3	2	yes
10.6.201.2. 123. udp	2	2	0	yes

-d オプション指定時

Real	Curcon	TotCon	RxPkts	TxPkts	RxBytes	T
------	--------	--------	--------	--------	---------	---

xBytes	PeakCon	Fail	Enable						
fd00:709::5.80.	tcp	865	3877	807	54618	122649	79		
572268	40	0	yes						
2001:380:283:710::4.69.	udp	1	3	30304	30292	15631008			
121168	2	0	yes						
10.6.201.2.123.	udp	2	2	14	7	672			
336	2	0	yes						

解**説** Address, Port, Proto

実サーバーの IP アドレス、ポート番号、プロトコルが表示されます。

MaxCon

実サーバーに設定されている最大接続数が表示されます。

Enable

実サーバーの設定状態です。有効の時は yes が表示されます。

Curcon

現在実サーバーに接続されている接続数の数が表示されます。

PeakCon

実サーバーに同時に接続されていた接続数のピーク値が表示されます。

TotCon

実サーバーに接続した接続数のトータル値が表示されます。

Fail

実サーバーがヘルスチェックにより DOWN と判定された累積の回数が表示されます。

RxPkts, TxPkts

実サーバーへ送信した、または実サーバーから受信したデータパケット数が表示されます。

データパケットとは、アプリケーションデータ付きのパケットを指します。

RxBytes, TxBytes

実サーバーへ送信した、または実サーバーから受信したデータパケットの処理サイズが表示されます。

データパケットとは、アプリケーションデータ付きのパケットを指します。

プロトコルが udp の場合、Curcon、PeakCon、TotCon は、処理したセッション数を表示します。

show route

機能 ルーティングテーブルを表示します。

フォーマット `show route [route-id <num>] [ipv4 | ipv6]`

パラメーター route-id

表示するルーティングテーブルのルート ID を指定します。

<num>

入力値範囲: 0 から 15

ipv4 | ipv6

表示するプロトコルを指定します。

実行例

```
netwiser> show route route-id 0
```

```
[route-id: 0]-----
Routing tables

Internet:
Destination      Gateway          Flags    Refs      Use    Mtu    Netif Expire
10.0.0.0/16      link#13         U        0        26837  1500  vlan100
10.0.100.65     link#13         UHS      0          0  16384    lo0
127.0.0.1       link#11         UH       0       87429  16384    lo0
172.16.21.0/24  10.6.201.8     UGS      0          0   1500  vlan100
172.16.22.0/24  10.6.201.9     UGS      0       26804  1500  vlan100
192.168.21.0/24 link#14         U        0        1093   1500  vlan200
192.168.21.66   link#14         UHS      0          0  16384    lo0

Internet6:
Destination      Gateway          Flags    Refs      Use    Mtu    Netif Expire
fd00::/64       link#15         U        0          64   1500  vlan300
fd00::10:197    link#15         UHS      0          0  16384    lo0
fd00::10:198    link#15         UHS      0          0  16384    lo0
fd00:708::/64   2001:380:283:710::8 UGS      0          5   1500  vlan100
fd00:709::/64   2001:380:283:710::9 UGS      0       26881  1500  vlan100
ff01::%vlan100/32 fe80::280:15ff:fed1:19c%vlan100 U        0          0   1500  vlan100
ff01::%vlan200/32 fe80::280:15ff:fed1:19c%vlan200 U        0          0   1500  vlan200
ff01::%vlan300/32 fe80::280:15ff:fed1:19c%vlan300 U        0          0   1500  vlan300
ff02::/16       ::1             UGRS     0          0  16384    lo0
ff02::%lo0/32   ::1             U        0          0  16384    lo0
```

- 解 説** IPv4、IPv6 ルーティングテーブルが表示されます。
- Destination
宛先ネットワークが表示されます。
- Gateway
宛先ネットワークへ到達するために使用されるネクストホップが表示されま
す。
- Flags
ルーティングテーブルの動作フラグが表示されます。

show running-config

機能 現在の設定状態を表示します。パラメーターを省略するとすべての設定情報を表示します。

フォーマット `show running-config [access-list [{ ip | ipv6 | mac } [<acl-name>]] | allow-ping | arp [aging-time] | buddy | debug | dns | hostname | interface { channel [<group-num>] | ethernet [<port-num>] | vlan [<vlan-id>] } | ipfw-list | logging | mac { address | aging-time | table-size } | name | nat-pool [<nat-pool-name>] | ndp | ntp | probe <probe-name> | proxy | real | reverse-nat | route | rule | snmp | spanning-tree | ssh | sync | telnet | user-mgmt | virtual [<virtual-name> | <virtual-id>] | vrrp | web-mgmt]`

パラメーター パラメーターを指定すると、設定ファイル中の指定された行のみを表示します。

実行例 1 `interface vlan` まで指定するとすべての VLAN インターフェイスが表示されま

す。

```
netwiser$ show running-config interface vlan
!  
interface vlan 1  
name default  
no ip address  
no ip redundant-address  
no ip virtual-address  
mtu 1500  
no rtadv  
no vrrp  
!  
interface vlan 100  
ip address 10.6.100.66/16  
ip address 2001:db8:710::66/64  
ip redundant-address 10.6.100.65  
ip redundant-address 2001:380:283:710::65  
ip virtual-address v-ext  
ip virtual-address v1  
mtu 1500  
no rtadv  
vrrp vrid 65  
no vrrp backup-l2forward  
!  
interface vlan 200  
ip address 192.168.21.66/24  
no ip redundant-address  
no ip virtual-address  
mtu 1500  
no rtadv  
no vrrp  
!
```

実行例 2 `interface vlan <vlan-id>`まで指定すると該当の VLAN インターフェイスのみが表示されます。

```
netwiser$ show running-config interface vlan 1
!  
interface vlan 1  
name default  
no ip address  
no ip redundant-address  
no ip virtual-address  
mtu 1500  
no rtadv  
no vrrp  
!
```

show session

機能 Layer4 セッションテーブルを表示します。

フォーマット show session

パラメーター なし

実行例

IPv4 Session Table

Proto	Client	Virtual	Real
tcp	10.0.1.1.34223	www1.http	server3.http
tcp	10.0.1.2.34775	www1.http	server2.http

...

IPv6 Session Table

Proto	Client	Virtual	Real
tcp	2001:db8::10.38887	WWW1.http	S
V1.http			
tcp	2001:db8::14.38887	WWW1.http	S
V4.http			

...

解説 全ての IP アドレスは name コマンドで設定された内容に置換されて表示されます。

Proto
udp または tcp が表示されます。

Client

クライアントの IP アドレス、ポート番号が表示されます。

Virtual

仮想サーバーの IP アドレス、ポート番号が表示されます。

Real

実サーバーの IP アドレス、ポート番号が表示されます。

show session-sync

機能 冗長構成でのセッション情報の同期に関する統計情報を表示します。

フォーマット show session-sync

パラメーター なし

実行例

```
L4 session sent = 289443
sticky sent     = 3272
cookie sent     = 0
L4 session rcvd = 164
sticky rcvd    = 35
cookie rcvd    = 0
socket error   = 1
```

解説 L4 session sent / rcvd
送受信が行われた L4 セッション情報数が表示されます。

sticky sent / rcvd
送受信が行われた IP セッション維持情報数が表示されます。

cookie sent / rcvd
送受信が行われたクッキーセッション維持情報数が表示されます。

socket error
接続の失敗等、セッション情報の送受信エラーの発生回数が表示されます。

show socket

機能 TCP/UDP セッションの接続状況を表示します。

フォーマット show socket

パラメーター なし

実行例

Active Internet connections

Proto	Recv-Q	Send-Q	Local Address	Foreign Address	(state)
tcp4	0	80	127.0.0.1.1023	127.0.0.1.41166	ESTABLISHED
tcp4	0	0	127.0.0.1.41166	127.0.0.1.1023	ESTABLISHED
tcp4	0	0	127.0.0.1.1023	*.*	LISTEN

解説 製品への管理アクセスで使用中のコネクションや、Layer7 負荷分散のセッションが表示されます。

Proto

tcp または udp でプロトコル、4 または 6 は IP バージョンを表します。

Recv-Q / Send-Q

送受信待ちのデータサイズが表示されます。

Local Address

本機器側の IP アドレスとポート番号が表示されます。

Foreign Address

相手側の IP アドレスとポート番号が表示されます。

state

TCP の接続状態が表示されます。

show spanning-tree

機能 スパニングツリーの状態を表示します。

フォーマット show spanning-tree

パラメーター なし

実行例

```
Root ID      32768.00:80:15:d1:00:3c
Root cost    0
Root port    0
Bridge ID    32768.00:80:15:d1:00:3c
Hello time   2
Max age      20
Forward delay 15
```

Interface	Port	Prio	Cost	Proto	State	Role	Link	Edge
port7	7	128	55	rstp	discard	disabled	shared	yes
port8	8	128	55	rstp	discard	disabled	shared	

解説 Root ID
スパニングツリーのルートブリッジの ID が表示されます。

Root cost
ルートブリッジまでのパスコストが表示されます。

Root port
ルートポートが表示されます。

Bridge ID
本機器のブリッジ ID が表示されます。

Hello time / Max age / Forward delay
ツリー内で使用されている HelloTime, MaxAge, ForwardDelay が表示されま
す。

イーサネットポートまたは論理ポート毎に下記の情報が表示されます。

Interface
イーサネットポートまたは論理ポート名が表示されます。

Port
ポートが使用するポート番号値が表示されます。

Prio / Cost

それぞれポートプライオリティー、ポートコストが表示されます。

Proto / State / Role

現在の STP の動作モード、ポートの状態、ポートロールが表示されます。

Link

ポートのリンク状態が表示されます。

Edge

Edge ポート指定されている場合 yes が表示されます。

show ssl

機能 証明書の有効性を SSL ポリシー毎に表示し、同時に統計情報も表示します。ポリシー名を指定し、ファイルの内容を表示することもできます。

フォーマット `show ssl [<policy-name> { cert | chain | client | crl }]`

パラメーター <policy-name>

ssl コマンドで設定したポリシー名を指定します。

cert

ポリシーにインストールされたサーバー証明書を表示します。

chain

ポリシーにインストールされた中間認証局証明書を表示します。

client

ポリシーにインストールされたクライアント認証用の認証局証明書を表示します。

crl

ポリシーが取得した証明書失効リストを表示します。

実行例 パラメーター省略時は SSL ポリシー毎に証明書の有効状態やインストールした秘密鍵の鍵長が表示されます。
total handshake 以降は技術サポートで使用する SSL アクセラレーション関連の統計情報が表示されます。

```
policy      cert  chain  client  key
common     valid  valid          4096
           valid
devel      valid  valid  valid  4096
           valid  valid
commerce   valid          valid  1024
NO-MATCH   bad key          secp384r1
```

```
ssl board option          = 1
total handshake           = 9
total RSA decrypt         = 9
total SSL connections     = 9
current SSL connections   = 0
current session           = 0
max SSL connections       = 1
max SSL sessions         = 4
```

```
MACed/encrypted AP data bytes = 2902
decrypted/MACed AP data bytes = 720
unexpected message             = 0
bad record mac                 = 0
record overflow                = 0
handshake failure              = 0
bad certificate                 = 0
unsupported certificate         = 0
certificate revoked             = 0
certificate expired             = 0
certificate unknown            = 0
decode failed                  = 0
decryption failed              = 0
protocol version                = 0
internal error.1               = 0
internal error.2               = 0
internal error.3               = 0
fatal alert rcvd               = 0
no renegotiation                = 0
unrecognized name              = 0
```

解 説 policy

SSL ポリシー名が表示されます。ポリシー名毎に下記の情報が表示されます。

cert

サーバー証明書がインポートされている場合 valid が表示されます。失効している場合は expired が表示されます。

証明書と秘密鍵が一致しない場合は bad key が表示されます。

chain

中間認証局の証明書がインポートされている場合 valid / expired / bad key が表示されます。

client

クライアント証明の認証局の証明書がインポートされている場合 valid / expired / bad key が表示されます。この欄に表示がある場合、システムはクライアント認証を有効にして動作します。

key

サーバー証明書に対応する秘密鍵の鍵長が表示されます。

show sticky

機能 セッション維持情報テーブルを表示します。

フォーマット show sticky { cookie | generic | ssl }

パラメーター cookie

クッキーセッション維持情報を表示します。

generic

ソース IP アドレスセッション維持情報を表示します。

ssl

SSL セッション ID セッション維持情報を表示します。

実行例 1 cookie: クッキーセッション維持情報を表示します。

Cookie Sticky Table(Server Address IPv4)

Real	Cookie	Expire
------	--------	--------

Cookie Sticky Table(Server Address IPv6)

Real	Cookie	Expire
S2v6. http	zA0iufalkse098aZlkjga	85
S2v6. http	000fjllh2390gbklnaOfwl3	85
S4v6. http	pp098Ai. z8ZZytTI83	167
S2v6. http	nmb82N8U-aaaJblkAQ	85

解説 1

Real

セッションが維持される対象の実サーバーIP アドレス、ポート番号が表示されます。

Cookie

実サーバーが発行したクッキー値が表示されます。

Expire

セッションが維持される残り時間が表示されます。

実行例 2 generic: IP アドレスセッション維持情報を表示します。

IP Sticky Table(Client Address IPv4)

Proto	Client	Virtual	Real	Expire
-------	--------	---------	------	--------

```
IP Sticky Table(Client Address IPv6)
Proto Client                               Virtual                                     R
eal                                          Expires
tcp 2001:380:283:707::184.0                2001:380:283:705::7.http                 S
4v6.http                                   555
tcp 2001:380:283:707::183.0                2001:380:283:705::7.http                 S
2v6.http                                   494
```

解説 2 Proto
tcp または udp が表示されます。

Client
セッションを維持するクライアントの IP アドレスを表示します。

Virtual
セッションが維持される対象の仮想サーバーIP アドレス、ポート番号が表示されます。

Real
セッションが維持される対象の実サーバーIP アドレス、ポート番号が表示されます。

Expires
セッションが維持される残り時間が表示されます。

実行例 3 ssl: SSL セッション ID のセッション維持情報を表示します。

```
SSL Sticky Table(Server Address IPv4)
Real          Session-ID          Expires
real_srv_apps_1.http 3a6ac265813810724fe97dc83fc1ce1cfe8b 19
192.168.47.210.https 3a6ac265813810724fe97dc83fc1ce1cfe9bf2ae3f6227b84d62e369101291e5 2592000
real_srv_apps_1.http 3a6ac265813810724fe97dc83fc1ce1cfe7b 1459
2001:0db8:bd05:01d2:288a:1fc0:0001:10ee.1433 3a6ac265813810724fe97dc83fc1ce1cfe9bf2ae3f6227b84d62e369101291e5 16
```

```
SSL Sticky Table(Server Address IPv6)
Real          Session-ID          Expires
real_srv_apps_1.http 3a6ac265813810724fe97dc83fc1ce1c 2592000
real_srv_apps_1.http 3a6ac265813810724fe97dc83fc1ce1cfe9bf2ae3f6227b84d62e369101291e5 2592000
2001:0db8:bd05:01d2:288a:1fc0:0001:10ee.1433 3a6ac265813810724fe97dc83fc1ce1cfe9bf2ae3f6227b84d62e369101291e5 2592000
```

解説 3 Real
セッションが維持される対象の実サーバーIP アドレス、ポート番号が表示され

ます。

Cookie

セッション維持に使用される SSL セッション ID が表示されます。

Expire

セッションが維持される残り時間が表示されます。

show system

機能 システムのリアルタイム統計情報を表示します。

フォーマット show system

パラメーター なし

実行例

```
total
% s= %u- | 10| 20| 30| 40| 50| 60| 70| 80| 90| 100|

CPU:          MEMORY:          SENSOR:          LB:
  0 %u+s      8 %use          40.0 deg C      0 L4 ssns
100 %idl      H/W SSL:        40 deg C(L)     0 L7 ssns
  0 %usr      48.9 deg C(R)  0 IP sticky
  0 %sys      0 L7 sticky

ETHER:        FORWARD:          TCP:          SSL:
  507 xpkt/s   0 L2fwd/s        112 con/s      0 curcons
16293 rpkt/s  0 L2fwdoct/s     6974 xpkt/s    0 maxcons
421026 xoct/s 1180 L2fld/s     729897 xoct/s  0 curssns
2215118 roct/s 272461 L2fldoct/s 6824 rpkt/s    0 maxssns
              0 IP4fwd/s       379245 roct/s  0 hnd/s
              0 IP4fwdoct/s   0 rsa/s
              0 IP6fwd/s      0 eoct/s
              0 IP6fwdoct/s  0 doct/s
```

Mon Sep 3 17:25:04 2018 interval: 5 (0.00)

解説 CPU: u+s, idl, usr, sys
システム全体の CPU 使用率、アイドルプロセスの CPU 使用率、プロセスの CPU 使用率、カーネルの CPU 使用率が表示されます。

MEMORY: use
メモリー使用率が表示されます。

SENSOR: deg C
CPU 温度が表示されます。

H/W SSL: deg C(L), deg C(R)
SSL 専用ボード搭載時には、ボード温度が表示されます。SSL 専用ボードが装

着されていない場合、'-'と表示されます。

LB: L4 ssns, L7 ssns, IP sticky, L7 sticky

L4 セッション数、L7 セッション数、IP セッション維持情報数、クッキーセッション維持情報数が表示されます。

ETHER: xpkt/s, rpkt/s, xoct/s, roct/s

送信パケット数毎秒、受信パケット数毎秒、送信バイト数毎秒、受信バイト数毎秒が表示されます。

FORWARD: L2fwd/s, L2fwdoct/s, L2fld/s, L2fldoct/s

L2 フォワードパケット数毎秒、L2 フォワードバイト数毎秒、L2 フラッドパケット数毎秒、L2 フラッドバイト毎秒が表示されます。

FORWARD: IP4fwd/s, IP4fwdoct/s, IP6fwd/s, IP6fwdoct/s

IPv4,v6 の L3 フォワードパケット数毎秒、L3 フォワードバイト数毎秒が表示されます。

TCP: con/s, xpkt/s, xoct/s, rpkt/s, roct/s

コネクション毎秒、送信パケット数・バイト数毎秒、受信パケット数・バイト数毎秒が表示されます。

SSL: curcons, maxcons, curssns, maxssns

現在の SSL コネクション数、最大コネクション数、現在保持している SSL セッション数、最大 SSL セッション数が表示されます。

SSL: hnd/s, rsa/s, eoct/s, doct/s

ハンドシェイク数毎秒、RSA 演算処理数毎秒、暗号化バイト数毎秒、復号化バイト数毎秒が表示されます。

show tech-support

機能 本機器の技術サポートを受ける場合に必要となるファイルを取り出します。

フォーマット show tech-support

パラメーター なし

解説 本コマンドでは **export tech-support** の簡易版が出力されます。

show traffic

機能 負荷分散に関連するトラフィック統計を表示します。

フォーマット show traffic

パラメーター なし

解説 本機器の技術サポートのために使用されるコマンドです。

show version

機能 フラッシュメモリーに保存されているファームウェアのバージョン情報を表示します。

フォーマット show version [primary | secondary | current]

パラメーター primary | secondary | current

primary または secondary 起動領域に保存されているファームウェアのバージョンを表示します。 **current** を指定すると現在動作中のファームウェアのバージョンを表示します。本パラメーターを省略した場合は **current** 動作となります。

実行例 1 パラメーターを省略、または **current** を指定すると起動時間やシリアル番号などの詳細な情報が表示されます。

```
netwiser> show version current
Firmware Version:      8.0.0(r777) built on 2018/10/10 19:30
Hardware Serial #:     8600019B
Model:                 SX-3940
Built-in Board:        SSL
```

```
System image file is "primary/netwiser-080000.bin"
System uptime is 3 days 9 hour 40 minutes 45 second
```

実行例 2 **primary** または **secondary** を指定するとファームウェアのバージョンのみが表示されます。

```
netwiser> show version secondary
8.0.0(r777) built on 2018/10/10 19:30
```

解説 **Firmware Version**
ファームウェアバージョンが表示されます。

Hardware Serial
機器のシリアル番号が表示されます。

Model
機器種別が表示されます。

Built-in Board
暗号演算のための専用ボードが装着されているか否かが表示されます。ボードが装着されている場合は"SSL"、そうでない場合は"---"と表示されます。

show virtual

機能 仮想サーバー毎の統計情報を表示します。

フォーマット `show virtual [<virtual-id>] [-r | -d]`

パラメーター <virtual-id>

表示させたい仮想サーバーID、または仮想サーバー名を指定します。
省略された場合、全仮想サーバーについて表示します。

-r

仮想サーバー情報を一行で表示させるためのオプションです。デフォルト表示と異なり、仮想サーバー情報を一行毎に表示します。

-d

仮想サーバー情報を一行で表示させるためのオプションです。**-r**に加え、より詳細な情報を表示します。

実行例 デフォルト表示 (**-r,-d** オプションなし)

```
Name: WWW1                Address: 10.6.100.100
                          Port: 80           Curcon: 0
                          Proto: tcp         PeakCon: 41
                          Enable: yes        TotCon: 141
```

```
Name: SSH-PROXY          Address: 10.6.100.100
                          Port: 60022       Curcon: 0
                          Proto: tcp         PeakCon: 1
                          Enable: yes        TotCon: 1
```

-r オプション指定時

```
Virtual                Curcon    TotCon  Fail  Enable
10.6.100.100.80.tcp    0      141    0     yes
10.6.100.100.60022.tcp 0      1      0     yes
```

-d オプション指定時

```
Virtual                Curcon    TotCon    RxPkts    TxPkts    RxBytes    T
xBytes PeakCon  Fail  Enable
10.6.100.100.80.tcp    0      141      807      54618    122649    79
572268    40    0     yes
10.6.100.100.60022.tcp 0      1        1        1        150
1212     1    0     yes
```

解説 Address, Port, Proto
仮想サーバーの IP アドレス、ポート番号、プロトコルが表示されます。

Enable

仮想サーバーの設定状態です。有効の時は yes が表示されます。

Curcon

現在仮想サーバーに接続されている接続の数が表示されます。

PeakCon

仮想サーバーに同時に接続されていた接続数のピーク値が表示されません。

TotCon

仮想サーバーに接続した接続数のトータル値が表示されます。

Fail

接続不良により仮想サーバーで破棄された接続の数が表示されます。

RxPkts, TxPkts

仮想サーバーがクライアントから受信した、またはクライアントへ送信したデータパケット数が表示されます。

データパケットとは、アプリケーションデータ付きのパケットを指します。

RxBytes, TxBytes

仮想サーバーがクライアントから受信した、またはクライアントへ送信したデータパケットの処理サイズが表示されます。

データパケットとは、アプリケーションデータ付きのパケットを指します。

show vlan

機能 各 VLAN に所属するイーサネットポートや論理チャネルの一覧を表示します。

フォーマット show vlan

パラメーター なし

実行例

VLAN	Name	State	Ports	Channel
1	default	up	1 4 7 8 9	
3	vlan_name_123456	up	2 3	2
trunk		up	10	

解説 VLAN
機器に設定された VLAN の VLAN ID が表示されます。 **tagged** 指定されたポートは trunk が表示されます。

Name

VLAN に設定した **name** が表示されます。

State

VLAN の動作状態が表示されます。

Ports

VLAN に所属しているイーサネットポートの一覧が表示されます。

Channel

VLAN に所属している論理チャネルの一覧が表示されます。

show vrrp

機能 VRRP の状態や関連する統計情報を表示します。

フォーマット show vrrp

パラメーター なし

実行例

```
instance 0
state          MASTER
priority       110
interval       100
preempt        Yes
master transitions = 1
backup transitions = 1
```

vrid	AdverSent	AdverRecvd	InvalidPacket
192	8820	0	0
191	8820	3	0

解説 instance
vrrp コマンドで設定したインスタンス番号が表示されます。

state
vrrp インスタンスの状態です。MASTER または BACKUP が表示されます。

priority
現在の VRRP プライオリティ値が表示されます。

interval
送信インターバルの設定値が表示されます。

preempt
preempt モードの設定です。有効の場合 Yes が表示されます。

master / backup transitions
MASTER または BACKUP に状態が変わった回数が表示されます。

vrid
設定された各 VRID 毎の統計情報が表示されます。

AdverSent / AdverRecvd
それぞれ VRRP 広告を送信した数、受信した数が表示されます。

InvalidPacket

不正な VRRP 広告を受信した数が表示されます。

特権モード

特権モードはグローバルモードから config コマンドで移行します。本機器の基本設定や、各種設定モードへの移行が可能です。複数ユーザがログインしている場合においては、特権モードに遷移できるのは 1 ユーザーのみとなります。

access-list

機能 各アクセスリスト設定モードに移動します。

フォーマット [no] access-list { mac | ipv4 | ipv6 } <list-name>

パラメーター mac

MAC アクセスリスト設定モードに移動します。

ipv4

IPv4 アクセスリスト設定モードに移動します。

ipv6

IPv6 アクセスリスト設定モードに移動します。

<list-name>

アクセスリスト名を指定します。リスト名が存在しない場合、新規のアクセスリストが生成されます。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

最大設定数: 128

advertise-mode

機能 GARP、UNA の送信を開始／停止します。

フォーマット `advertise-mode { on | off }`

パラメーター `on, off`

GARP、UNA の送信を開始する場合 `on` を、停止する場合 `off` を指定します。
`on` を指定後、10 分経過すると自動で停止します。

allow-ping

機能 仮想サーバーへの ping を許可します。

フォーマット [no] allow-ping

パラメーター なし

解説 no を指定すると仮想サーバーへの ping が禁止されます。（デフォルト動作）

arp

機能 ARP テーブルに関する設定を行います。

フォーマット [no] arp <ipv4-addr> <mac-addr>
[no] arp aging-time <time-expression (dhm)>

パラメーター <ipv4-addr> <mac-addr>
静的 ARP エントリーを追加するホストの IPv4 アドレスと、それに対応する MAC のアドレスを指定します。
最大設定数: 128

aging-time <time-expression (dhm)>
生存時間を時間または分単位で設定します。例えば 1h(1 時間)、30m(30 分)、2h50m(2 時間 50 分)、という表記が可能です。
デフォルト: 20 分
設定範囲: 1 分から 1 日

buddy

機能 IP アドレスセッション維持グループを形成します。

フォーマット [no] **buddy** <buddy-name> <virtual-id>

パラメーター <buddy-name>

セッション維持グループ名を指定します。リスト名が存在しない場合、新規のグループが形成されます。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

<virtual-id>

グループに追加する仮想サーバーID、または仮想サーバー名を指定します。

仮想サーバーIDの説明は **virtual** コマンドの説明を参照してください。

解説 **no** を指定すると IP アドレスセッション維持グループから仮想サーバーを削除します。

一つのグループには五つまでの仮想サーバーを登録することができます。

仮想サーバーは複数のグループに参加することはできません。

注意 **buddy** コマンドで形成したグループは、IP アドレスセッション維持(**sticky generic**)でのみ有効となります。

HTTP Cookie によるセッション維持でグループを作る場合には、同じ Cookie 名で Cookie セッション維持を設定してください。

cert-update

機能 SSL 証明書自動更新を形成します。

フォーマット [no] cert-update <prefix>

パラメーター <prefix >

自動更新したい SSL ポリシー名を指定します。
prefix の後に _XXX (アンダーバーと数字) にマッチする SSL ポリシー名があった場合は、それも自動更新対象となります。
XXX が数値以外のものは対象外です。

解説 no を指定すると SSL 証明書自動更新を削除します。
※SSL ポリシーはダウンロード前の中途半端な状態であってもそのまま残ります。

注意 自動更新対象は prefix または prefix_XXX にマッチする SSL ポリシーです。以降この XXX 値をインデックス値と称します。(prefix のみは 0 扱い)
インデックス値が一番大きいものが最新の SSL ポリシーと判断し、証明書の有効期限を監視します。
期限切れが近づくとインデックス値+1 の新しい SSL ポリシーを作成し、そこに CSR 作成、証明書のダウンロードをして行きます。
CSR 無しモードでは正常な鍵と証明書のダウンロードが完了すると、直ちに次のダウンロード用にインデックス値+1 の新しい SSL ポリシーを作成します。
設定の詳細は SSL 証明書自動更新設定モードを参照してください。

clear access-log

機能 機器内部に保存されている cloud-waf のアクセスログを削除します。

フォーマット clear access-log

パラメーター なし

clear arp

機能 動的に生成された ARP テーブルエントリを削除します。

フォーマット `clear arp [<ipv4-addr>]`

パラメーター <ipv4-addr>
IP アドレスを指定すると、指定した IP アドレスのエントリのみを削除します。

解説 IP アドレスを省略した場合は、すべての動的エントリが削除されます。

clear config

機能 機器に保存されている設定情報を削除します。

フォーマット `clear config { all | primary | secondary | current }`

パラメーター **all**
機器の設定を工場出荷状態に戻します。

primary
primary 領域の設定情報のみを削除します。

secondary
secondary 領域の設定情報のみを削除します。

current
現在の起動領域の設定情報のみを削除します。

解説 本コマンドは **write erase** コマンドと同様の動作を行います。

clear content

機能 インポートしたソーリーコンテンツファイルを削除します。

フォーマット `clear content <content-name>`

パラメーター `<content-name>`
インポート時に指定したソーリーコンテンツ名を指定します。

clear logging

機能 機器内部に保存されているログを削除します。

フォーマット clear logging

パラメーター なし

clear login-session

機能 現在ログインしているユーザーを強制的にログアウトさせます。

フォーマット `clear login-session <terminal-id>`

パラメーター `<terminal-id>`
ログアウトさせるユーザーの端末 ID を指定します。

解説 端末 ID は `show login-session` コマンドの Term-ID で確認することができます。

clear mac

機能 動的に生成されたフォーワーディングデータベース(FDB)を削除します。

フォーマット `clear mac [<mac-addr>]`

パラメーター <mac-addr>
MAC アドレスを指定すると、指定した MAC アドレスのエントリーのみを削除します。

解説 MAC アドレスを省略した場合は、すべての動的エントリーが削除されます。

clear packet-trace

機能 機器内部に保存されている L2/L7 パケットトレースデータを削除します。

フォーマット clear packet-trace

パラメーター なし

解説 本機器がパケットトレース機能により保存したキャプチャデータを全て削除します。

clear ssl-session

機能 機器内部に保存されている SSL セッションを削除します。

フォーマット clear ssl-session

パラメーター なし

解説 本機器が SSL アクセラレーション機能で生成した SSL セッション情報をすべて削除します。
WEB/UI で HTTPS アクセスした際に生成された SSL セッション情報は削除されません。

clear statistics

機能 各種統計情報をクリアします。

フォーマット `clear statistics { ethernet | l2forward | session | ssl | vrrp | session-sync | probe }`
`clear statistics { virtual [<virtual-id>] | real [<real-id>] }`

パラメーター **ethernet**

イーサネットの統計情報をクリアします。

l2forward

L2 フォワーディング、L2 フラッディングの統計情報をクリアします。

session

負荷分散に関連する統計情報をクリアします。(例. L4 セッション数、セッション維持情報数など)

ssl

SSL アクセラレーションに関する統計情報をクリアします。

vrrp

VRRP に関連する統計情報をクリアします。

session-sync

冗長構成でのセッション情報の同期やコマンド情報の同期に関する統計情報をクリアします。

probe

サーバーヘルスチェックの成功数、失敗数などの統計情報をクリアします。

virtual

仮想サーバーが保持している統計情報をクリアします。

<virtual-id>

仮想サーバーID を指定すると、指定した仮想サーバーID に関連した統計情報のみをクリアします。

省略した場合は、全ての仮想サーバーの統計情報をクリアします。

real

実サーバーが保持している統計情報をクリアします。

<real-id>

実サーバーID を指定すると、指定した実サーバーID に関連した統計情報のみ

をクリアします。
省略した場合は、全ての実サーバーの統計情報をクリアします。

cloud-waf

機能 クラウド WAF の設定を行います。

フォーマット [no] cloud-waf manager-address <ipv4-addr> port <port-num>
[no] cloud-waf key <string>

パラメーター manager-address <ipv4-addr>

クラウド WAF マネージャーの IPv4 アドレスを設定します。

port <port-num>

クラウド WAF マネージャーの宛先ポート番号を設定します。

key <string>

クラウド WAF マネージャーより発行されたエージェントキー文字列を設定します。

入力値範囲: 1 から 256 文字

注意 クラウド WAF が有効の場合、manager-address と key の設定変更することは出来ません。
設定変更する場合は一度クラウド WAF を無効にする必要があります。

copy

機能 設定ファイルやファームウェアを起動領域間でコピーします。

フォーマット `copy running-config startup-config`
`copy startup-config { primary secondary | secondary primary }`
`copy firmware { primary secondary | secondary primary }`

パラメーター **running-config**
現在動作中の設定情報です。**running-config** は現在の起動領域にのみ保存することができます。

startup-config
機器の起動時に適用される設定情報です。primary、secondary 領域間で相互にコピーすることができます。

firmware
機器のファームウェアファイルです。primary、secondary 領域間で相互にコピーすることができます。

primary secondary
primary 領域から secondary 領域にコピーします。

secondary primary
secondary 領域から primary 領域にコピーします。

解説 現在の起動領域は **show version** コマンドによって確認することができます。

date

機能 日時を設定します。

フォーマット `date` [yyyy]mm]dd]HH]MM[.ss]

パラメーター *cc, yy, mm, dd, HH, MM, .ss*

西暦の上 2 桁、下 2 桁、月、日、時間、分、秒をそれぞれ指定します。*MM* を省略することはできません。

実行例

```
netwiser (config)# date 1420
Mon Aug  4 14:20:00 JST 2018
netwiser (config)# date 051420
Tue Aug  5 14:20:00 JST 2018
```

dns

機能 DNS サーバーを設定します。

フォーマット [no] dns { primary | secondary } <ip-addr>

パラメーター primary

プライマリDNS サーバーを設定します。

secondary

セカンダリDNS サーバーを設定します。

<ip-addr>

DNS サーバーの IP アドレスを指定します。

enable cloud-waf

機能 クラウド WAF を有効化します。

フォーマット [no] enable cloud-waf

パラメーター なし

注意 manager-address と key が設定されていない場合、クラウド WAF は有効になりません。

enable probe

機能 ヘルスチェックエントリーを有効化します。

フォーマット [no] enable probe <probe-name>

パラメーター <probe-name>
probe コマンドで設定したヘルスチェック名を指定します。

解説 本コマンドは probe 設定モードで [no] enable するのと同じ効果があります。

enable real

機能 実サーバーを有効化します。

フォーマット [no] **enable real** { <real-ip-addr> | <real-id> }

パラメーター <real-ip-addr>

real コマンドで設定した実サーバーのうち IP アドレスが一致するエントリーすべてを有効化します。

<real-id>

real コマンドで設定した実サーバーID を指定します。

enable reverse-nat

機能 リバース NAT エントリーを有効化します。

フォーマット [no] enable reverse-nat <nat-pool-id>

パラメーター <nat-pool-id>
reverse-nat コマンドで設定したリバース NAT ID を指定します。

解説 本コマンドは reverse-nat 設定モードで [no] enable するのと同じ効果があります。

enable virtual

機能 仮想サーバーを有効化します。

フォーマット [no] enable virtual { <virtual-ip-addr> | <virtual-id> }

パラメーター <virtual-ip-addr>

virtual コマンドで設定した仮想サーバーのうち IP アドレスが一致するエントリーすべてを有効化します。

<virtual-id>

virtual コマンドで設定した仮想サーバーID を指定します。

解説 本コマンドは virtual 設定モードで [no] enable するのと同じ効果があります。

halt

機能 システムをシャットダウンします。

フォーマット halt

パラメーター なし

hostname

機能 本機器のホスト名を設定します。

フォーマット `hostname <host-name>`

パラメーター `<host-name>`

ホスト名を設定します。

デフォルト: netwiser

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、ハイフン(-)、アンダーバー(_)を使用することはできません

import all

機能 システムが動作するために必要な全ての設定情報を機器に投入します。

フォーマット `import all [primary | secondary | current] [tftp | zmodem]`

パラメーター `primary | secondary | current`

`primary` または `secondary` 起動領域に設定情報を投入します。`current` を指定すると現在の起動領域へファイルを投入します。省略時には `current` となります。

`tftp | zmodem`

`tftp` または `zmodem` によってファイルを投入します。省略時には `tftp` 動作となります。

解説 現在の起動領域は `show version` コマンドによって確認することができます。

import config

機能 テキスト形式の設定情報ファイルを機器に投入します。

フォーマット `import config [primary | secondary | current] [tftp | zmodem]`

パラメーター `primary | secondary | current`

`primary` または `secondary` 起動領域に設定情報を投入します。`current` を指定すると現在の起動領域へファイルを投入します。本パラメーターを省略した場合は `current` となります。

`tftp | zmodem`

`tftp` または `zmodem` によってファイルを投入します。省略時には `tftp` 動作となります。

解説 現在の起動領域は `show version` コマンドによって確認することができます。機器を動作させるためには SSL 関連の鍵・証明書などのファイル、HTML コンテンツなどが別途必要になる場合があります。

import content

機能 ソーリーコンテンツを機器に投入します。

フォーマット `import content <content-name> [tftp | zmodem]`

パラメーター `<content-name>`

コンテンツの識別用に名称を設定します。

コンテンツ名に使用できる文字は半角のアルファベット、数字、ハイフン(-)、アンダーバー(_)です。

16文字までの文字列で先頭文字に数字、ハイフン(-)、アンダーバー(_)を使用することはできません。

tftp | zmodem

tftp または zmodem によってファイルを投入します。省略時には **tftp** 動作となります。

解説 `<content-name>`は **bind** コマンドによって仮想サーバーに割り当てる際に使用します。

注意 ソーリーコンテンツのファイルサイズは最大 4500 バイトに制限されます。4500 バイトを超えるコンテンツは適切に表示されませんのでご注意ください。

import firmware

機能 ファームウェアを機器に投入します。

フォーマット `import firmware [primary | secondary | current] [tftp | zmodem]`

パラメーター `primary | secondary | current`

`primary` または `secondary` 起動領域に設定情報を投入します。 `current` を指定すると現在の起動領域へファームウェアを投入します。本パラメーターを省略した場合は `current` となります。

`tftp | zmodem`

`tftp` または `zmodem` によってファームウェアを投入します。省略時には `tftp` 動作となります。

解説 現在の起動領域は `show version` コマンドによって確認することができます。

import licensekey

機能 NetwiserVE EP 版のアクティベート用認証 KEY を機器に投入します。

フォーマット import licensekey [tftp | http]

パラメーター tftp | http
tftp または *http* によって認証 ID を投入します。省略時は *tftp* 動作となります。

MEMO このコマンドは非公開コマンドです。

import ssl

機能 SSL アクセラレーションで使用する鍵や証明書を機器に投入します。

フォーマット `import ssl <ssl-name> { cert | chain | client | key | pkcs12 } [tftp | zmodem | tftp-get { <ipv4-addr> | <host-name> }]`

パラメーター `<ssl-name>`
config モードの `ssl` コマンドで設定した `<ssl-name>` を指定します。

cert
サーバー証明書を投入します。

chain
中間 CA 証明書を投入します。2 枚まで投入することができます。

client
クライアント認証で使用する CA 局の証明書を投入します。2 枚まで投入することができます。

key
`cert` と対になる秘密鍵を投入します。

pkcs12
サーバー証明書、中間 CA 局証明書、秘密鍵をまとめて PKCS#12 形式で投入します。

`tftp | zmodem | tftp-get { <ipv4-addr> | <host-name> }`
tftp または zmodem によってファイルを投入します。
`tftp-get` を指定した場合、送信先 IPv4 アドレスまたはホスト名を指定する必要があります。
省略時には `tftp` 動作となります。

import webconf

機能 WEB 管理画面の表示/非表示状態を記述したテキスト形式の設定情報ファイルを機器に投入します。

フォーマット import webconf [tftp | zmodem]

パラメーター tftp | zmodem
tftp または zmodem によってファイルを投入します。省略時には **tftp** 動作となります。

interface

機能 各種設定モードに移動します。

フォーマット `interface ethernet <port-num>`
`interface channel <group-num>`
`[no] interface vlan <vlan-id>`

パラメーター `ethernet <port-num>`
イーサネット設定モードに移動します。
<port-num>にはイーサネットポートのポート番号を指定します。

`channel <group-num>`
論理チャネル設定モードに移動します。
<group-num>には論理チャネル番号を指定します。

`vlan <vlan-id>`
VLAN 設定モードに移動します。該当の VLAN ID が存在しない場合は VLAN を追加します。
<vlan-id>は 1 から 4094 の数字を指定します。vlan1 は削除することができません。

解説 `no` を指定すると VLAN インターフェイスを削除することができます。
<port-num> は「1,2,3」、「2-10」、「1,4-6」のように複数を同時に選択することができます。

注意 <port-num>、<group-num>に指定する数字はご使用の機器のイーサネットポート数によって異なります。
<group-num>の入力値制限についてはイーサネット設定モードの `channel` をご参照ください。

ipfw-list

機能 各 IPFW リスト設定モードに移動します。

フォーマット [no] ipfw-list { ethport | vlan } <list-name>

パラメーター ethport

IPFW イーサネットポート設定モードに移動します。

vlan

IPFW VLAN 設定モードに移動します。

<list-name>

IPfw リスト名を指定します。リスト名が存在しない場合、新規の IPFW リストが生成されます。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

最大設定数: 128

l2-trace

機能 L2 パケットをトレースし、結果を pcap 形式のファイルで保存します。保存した pcap ファイルは、WEB 管理画面または **export tech-support** コマンドにて取得できます。
本コマンドと packet-trace コマンドを同時に実行することは出来ません。

フォーマット l2-trace on [rx | tx] ethernet <port-num>
l2-trace on permit ip [<ip-address>] ethernet <port-num>
l2-trace off

パラメーター on, off

トレース処理を開始する場合 **on** を、停止する場合 **off** を指定します。
パケットトレースを停止した時点でキャプチャデータを圧縮するため、トレースの停止処理が完了するまでに数十秒～1 分程度の時間を要する場合があります。

rx, tx

rx の場合、受信パケット情報のみキャプチャファイルに保存します。
tx の場合、送信パケット情報のみキャプチャファイルに保存します。
省略された場合、送受信 L2 パケット情報をキャプチャデータに保存します。

ip <ip-address>

IP アドレスでフィルターリングしたい場合、任意のアドレスを入力します。
送信元アドレス、宛先アドレスのいずれも検索対象となります。
アドレスが省略された場合、全ての IP パケット情報をキャプチャファイルに保存します。

ethernet <port-num>

パケットトレースを行うイーサネットポートのポート番号を入力します。

注意 本コマンドは解析用コマンドであり、使い方によって、disk の消耗速度を早める危険性があります。
使用する場合は必ず、弊社技術サポートエンジニアの指示の下で使用してください。
l2-trace コマンドと packet-trace コマンドを同時に実行することは出来ません。

logging

機能 システムログの設定を変更します。

フォーマット [no] logging output <facility.level>
[no] logging host <ip-addr>
[no] logging mail-host <ip-addr> <mail-level>
[no] logging { from | reply-to | to } <mail-addr>
logging test-log [<level>]

パラメーター output <facility.level>

facility: SYSLOG のファシリティとレベルを 16 から 23 の数字で指定します。数字はそれぞれ LOCAL0 から LOCAL7 を意味します。

level: SYSLOG レベルを 0 から 7 の数字で指定します。数字が小さいほど重大なログであることを意味します。

host <ip-addr>

SYSLOG サーバーの IP アドレスを指定します。

最大設定数: 4

mail-host <ip-addr>

SMTP サーバーの IP アドレスを指定します。

<mail-level>

SYSLOG レベルを指定します。このレベル以下のログがメールとして送信されます。

from <mail-addr>

SYSLOG メールを送信元アドレスを指定します。

reply-to <mail-addr>

SYSLOG メール返信先アドレスを指定します。

to <mail-addr>

SYSLOG メール宛先を指定します。

最大設定数: 16

test-log [<level>]

実行したタイミングでテスト用ログを出力します。

level: テスト用に出力するログの SYSLOG レベルを 0 から 7 の数字で指定します。省略した場合 5(NOTICE)がセットされます。

mac

機能 MAC アドレステーブルに関する設定を行います。

フォーマット [no] **mac address** <mac-addr> { **channel** <group-num> | **ethernet** <port-num> } [**vlan** <vlan-id>]
[no] **mac aging-time** <time-expression (hm)>
[no] **mac table-size** <table-num>

パラメーター **address** <mac-addr>

静的 MAC アドレステーブルを生成する MAC アドレスを指定します。
最大設定数: 128

channel <group-num>

論理チャンネル番号 <group-num> に静的 MAC アドレスを設定します。

ethernet <port-num>

イーサネットポート番号 <port-num> に静的 MAC アドレスを設定します。

vlan <vlan-id>

対象のポートが **tagged** に指定されている場合、オプションで VLAN ID を指定します。

aging-time <time-expression (hm)>

動的 MAC アドレステーブルエントリーの生存時間を設定します。
分単位で指定します。例えば 1m(1 分)、1h(1 時間)、という表記が可能です。
デフォルト: 20 分
設定範囲: 1 分(1m)から 120 分(2h)

table-size <table-num>

MAC アドレステーブルエントリーの最大数を設定します。
デフォルト: 1024
設定範囲: 1 から 4096

maxconns

機能 実サーバーへの接続の最大数を設定します。

フォーマット [no] maxconns <real-id> <connection-num>

パラメーター <real-id>
接続数を制限する実サーバーの ID を指定します。

<connection-num>
確立できる接続の最大値を指定します。
デフォルト: 無制限(0)
設定範囲: 0 から 65535

name

機能 IP アドレスに名前付けします。

フォーマット [no] name <ip-addr-name>{ <ipv4-addr>| <ipv6-addr>}

パラメーター <ip-addr-name>

IP アドレス名を入力します。IP アドレス名 **any** はシステムにより予約されています。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

<ipv4-addr>

IP アドレス名と対応付ける IPv4 アドレスを指定します。

<ipv6-addr>

IP アドレス名と対応付ける IPv6 アドレスを指定します。

最大設定数: 512

解説 **name** コマンドで設定した IP アドレス名は他のコマンドで IP アドレスの代わりに使用することができます。

nat-log

機能 負荷分散によって変換された IP アドレスのログを外部ホストに送信します。

フォーマット [no] nat-log <ip-addr> <facility.level>

パラメーター <ip-addr>

SYSLOG サーバーの IP アドレスを指定します。

<facility.level>

facility: SYSLOG のファシリティを 16 から 23 の数字で指定します。数字はそれぞれ LOCAL0 から LOCAL7 を意味します。

level: SYSLOG レベルを 0 から 7 の数字で指定します。数字が小さいほど重大なログであることを意味します。

解説 nat-log はシステムに一つだけ登録することができます。

nat-pool

機能 NAT プール設定モードに移動します。

フォーマット [no] nat-pool <nat-pool-name>

パラメーター <nat-pool-name>

NAT アドレスプール名を指定します。プール名が存在しない場合、新規のアドレスプールが生成されます。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

解説 <nat-pool-name>は **reverse-nat** コマンドや **source-nat** コマンドで NAT アドレスプールを指定する際に使用します。

ndp

機能 静的 NDP テーブルを設定します。

フォーマット [no] ndp <ipv6-addr> <mac-addr>

パラメーター <ipv6-addr> <mac-addr>

静的 NDP エントリーを追加するホストの IPv6 アドレスと、それに対応する MAC がアドレスを指定します。

最大設定数: 128

ntp

機能 NTP サーバーを設定します。

フォーマット [no] ntp <ip-addr>
[no] ntp restrict

パラメーター <ip-addr>
NTP サーバーの IP アドレスを指定します。
最大設定数: 4

restrict
設定した NTP サーバー以外との時刻情報の交換を行いません。

packet-trace

機能 L7 負荷分散パケットをトレースし、結果を pcap 形式のファイルで保存します。
保存した pcap ファイルは、WEB 管理画面または **export tech-support** コマンドにて取得できます。
本コマンドと l2-trace コマンドを同時に実行することは出来ません。

フォーマット `packet-trace on [{ deny | permit } ip <ip-address>]`
`packet-trace on [{ deny | permit } port <num>]`
`packet-trace on [{ deny | permit } ip <ip-address> port <num> [and-policy | or-policy]]`
`packet-trace off`

パラメーター on, off

トレース処理を開始する場合 **on** を、停止する場合 **off** を指定します。
パケットトレースを停止した時点でキャプチャデータを圧縮するため、トレースの停止処理が完了するまでに数十秒～1 分程度の時間を要する場合があります。

deny, permit

フィルタールールを設定する場合選択します。

deny の場合、任意のフィルタールールに合致しないパケット情報のみキャプチャファイルに保存します。

permit の場合、任意のフィルタールールに合致するパケット情報のみキャプチャファイルに保存します。

省略された場合、全ての L7 負荷分散パケットをキャプチャデータに保存します。

ip <ip-address>

IP アドレスでフィルターリングしたい場合、任意のアドレスを入力します。
送信元アドレス、宛先アドレスのいずれも検索対象となります。

port <num>

ポート番号でフィルターリングしたい場合、任意のポート番号を入力します。
送信元ポート番号、宛先ポート番号のいずれも検索対象となります。

and-policy, or-policy

IP アドレス、ポート番号の両方をフィルタールールに含める場合、二つのフィルター情報の組み合わせ条件を指定します。

AND 条件であれば **and-policy**、OR 条件であれば **or-policy** を指定します。

省略された場合、AND 条件が適用されます。

- 注 意** 本コマンドは解析用コマンドであり、使い方によって、disk の消耗速度を早める危険性があります。
使用する場合は必ず、弊社技術サポートエンジニアの指示の下で使用してください。
l2-trace コマンドと packet-trace コマンドを同時に実行することは出来ません。

probe

機能 実サーバーへのヘルスチェックを設定します。

フォーマット [no] probe <probe-name> <ip-addr>[.<port>.{udp|tcp|ssl}]
[no] probe <probe-name> <nested-expression>

パラメーター <probe-name>

ヘルスチェック識別用に名前を設定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

<ip-addr>

ヘルスチェック対象の IP アドレスを指定します。

IP アドレス以降を省略した場合、自動的に ICMP echo によるヘルスチェック動作を行います。

<port>

TCP または UDP のポート番号を指定します。

udp|tcp|ssl

それぞれ UDP、TCP、SSL のヘルスチェックが動作します。

<nested-expression>

複数のヘルスチェックを組み合わせた式を記述します。

式は<probe-name>と「&&」AND, 「||」OR, 「()」括弧を組み合わせて表現します。

式の記号はスペースで区切る必要があります。

最大設定数: 1024

説明 <ip-addr>、<port>、プロトコルの間にはスペースを入れることはできません。
それぞれドット「.」で区切って指定してください。

proxy

機能 プロキシサーバーを設定します。

フォーマット [no] proxy <ip-addr> <port>

パラメーター <ip-addr>
プロキシサーバーの IP アドレスを指定します。

<port>
プロキシサーバーのポート番号を指定します。

解説 本設定は CRL の取得で外部のウェブサーバーにアクセスする際に必要となる場合があります。

real

機能 実サーバーを定義します。

フォーマット [no] real <ip-addr>.<port>.{udp|tcp}

パラメーター <ip-addr>

実サーバーの IP アドレスを指定します。

<port>

TCP または UDP のポート番号を指定します。0(ゼロ)は任意のポート番号を意味します。

udp|tcp

それぞれ UDP、TCP の実サーバーを定義します。

最大設定数: IPv4, IPv6 それぞれ最大 256

解説 <ip-addr>、<port>、プロトコルの間にはスペースを入れることはできません。
それぞれドット「.」で区切って指定してください。
本製品では「<ip-addr>.<port>.プロトコル」で指定した文字列をサーバーIDと呼びます。

reboot

機能 システムを再起動します。

フォーマット `reboot [primary | secondary]`

パラメーター `primary | secondary`

それぞれ再起動後の起動領域が `primary` 領域、`secondary` 領域となります。
パラメーターを省略した場合は現在の起動領域のまま再起動します。

解説 現在の起動領域は `show version` コマンドによって確認することができます。

reverse-nat

機能 リバース NAT 設定モードに移動します。リバース NAT 定義が存在しない場合はリバース NAT 設定を新規に追加します。

フォーマット [no] reverse-nat <nat-pool-name>.<port>.{ ftp | tcp | udp }

パラメーター <nat-pool-name>

nat-pool コマンドで設定した NAT アドレスプール名を指定します。

<port>

TCP または UDP のポート番号を指定します。

0(ゼロ)は任意のポート番号を意味します。

ftp | udp | tcp

アドレス変換を行うプロトコルを選択します。

FTP を NAT する場合は **ftp** を指定してください。

最大設定数: IPv4, IPv6 合わせて最大 256 まで設定可能

解説 <nat-pool-name>、<port>、プロトコルの間にはスペースを入れることはできません。
それぞれドット「.」で区切って指定してください。

route

機能 静的ルートを追加します。

フォーマット [no] route <ipv4-dst-network> { <ipv4-dst-mask> | </ipv4-dst-masklen> }
<gateway-ipv4-addr> [id <num>]
[no] route <ipv6-dst-network> </ipv6-prefixlen> <gateway-ipv6-addr>
[id <num>]

パラメーター <ipv4-dst-network>

IPv4 の宛先ネットワークを指定します。

<ipv4-dst-mask>

宛先ネットワークのネットマスクを.(ドット)区切りの表記で指定します。

</ipv4-dst-masklen>

宛先ネットワークのネットマスクのビット長を/(スラッシュ)に続けて指定します。

<gateway-ipv4-addr>

ルーターの IPv4 アドレスを指定します。

<ipv6-dst-network>

IPv6 の宛先ネットワークを指定します。

</ipv6-prefixlen>

宛先ネットワークのプレフィクス長を/(スラッシュ)に続けて指定します。

<gateway-ipv6-addr>

ルーターの IPv6 アドレスを指定します。

id

登録する静的ルートのルーティングテーブルの ID を指定します。

<num>

入力値範囲: 0 から 15

最大設定数: IPv4, IPv6 それぞれ最大 128

rule

機能 HTTP 負荷分散のスイッチングルールを設定します。

フォーマット [no] rule <rule-name> { host | method | path | user-agent } <"string">
[no] rule <rule-name> <"nested-expression">
[no] rule <rule-name> location { http | https } <"domain"> <"path">

パラメーター <rule-name>

スイッチングルールの識別用に名前を設定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

host <"string">

HTTP リクエストヘッダーの Host ヘッダー値によるスイッチングを行います。

(例. www.seiko-sol.co.jp、example.com)

method <"string">

HTTP リクエストヘッダーのメソッドによるスイッチングを行います。

(例. GET、POST)

path <"string">

HTTP リクエストヘッダーのリクエストパスによるスイッチングを行います。

(例. /cgi-bin/*、/login)

user-agent <"string">

HTTP リクエストヘッダーの User-Agent ヘッダー値によるスイッチングを行います。

(例. *Mozilla*、*MSIE*)

<"string">

指定する文字列は"(ダブルクォーテーション)で挟む必要があります。

method が指定された場合を除き、文字列には*(ワイルドカード)を使用することができます。

(例. string*(前方一致)、*string(後方一致)、*string*(部分一致))

<"nested-expression">

複数のスイッチングルールを組み合わせた式を記述します。

式は<rule-name>と「&&」AND, 「||」OR, 「()」括弧を組み合わせて表現します。

式の記号はスペースで区切る必要があります。

location

サーバーのリダイレクト応答に含まれる Location ヘッダーを置換するためのルールを定義します。

http

リダイレクト先が http である場合に指定します。

https

リダイレクト先が https である場合に指定します。

<"domain">

リダイレクト先のドメインを指定します。

すべてに一致するドメインとして*(アスタリスク)を指定することもできます。ドメインは"(ダブルクォーテーション)で挟んで表記する必要があります。

<"path">

リダイレクト先のパスを指定します。

すべてに一致するパスとして*(アスタリスク)を指定することもできます。パスは"(ダブルクォーテーション)で挟んで表記する必要があります。

最大設定数: 1024

snmp

機能 SNMP 関連の設定を行います。

フォーマット [no] snmp host <ipv4-addr> [version { 1 | 2c }]
[no] snmp community <"string">
[no] snmp contact <"string">
[no] snmp location <"string">
[no] snmp trap trigger <"string"> [once]
[no] snmp trap agent-address vlan <vlan-id>
[no] snmp trap link-updown-delay <time-expression>

パラメーター host <ipv4-addr>

SNMP マネージャーの IPv4 アドレスを設定します。
最大設定数: 4

version { 1 | 2c }

SNMP マネージャーが対応している SNMP バージョンを選択します。

community <"string">

SNMP コミュニティ名を設定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)が使用可能

入力値範囲: 1 から 16 文字

その他: 先頭文字に数字を使用することはできません

contact <"string">

mib-2.system.sysContact を取得したときの値を設定します。

入力値制限: "(ダブルクォート)、\"(バックスラッシュ/円記号)を除く半角英数
記号文字が使用可能

入力値範囲: 1 から 256 文字

location <"string">

mib-2.system.sysLocation を取得したときの値を設定します。

入力値制限: "(ダブルクォート)、\"(バックスラッシュ/円記号)を除く半角英数
記号文字が使用可能

入力値範囲: 1 から 256 文字

trap trigger <"string">

syslog の文字列を設定します。<"string">にマッチしたログが出力されると、
連動して SNMP Trap がマネージャーに送信されます。

最大設定数: 16

once

ログが連続して出力された場合、最初の 1 回目のみ Trap を送信します。

trap agent-address vlan <*vlan-id*>

SNMPv1 トラップ発行時のエージェントアドレスを設定します。

指定した VLAN に設定されている IPv4 管理アドレスがエージェントアドレスとして使用されます。

trap link-updown-delay <*time-expression*>

リンクアップまたはリンクダウン時に発生する SNMP トラップの送信を、指定した秒数だけ遅らせることが可能です。

デフォルト: 0

設定範囲: 0 から 10 秒

注 意 IPv6 の SNMP マネージャーからのアクセスには対応していません。

spanning-tree

機能 機器全体に反映されるスパンニングツリーの設定を行います。

フォーマット [no] spanning-tree [master | backup] priority <bridge-priority>
[no] spanning-tree { hello-time | forward-delay | max-age } <time-expression(s)>

パラメーター master | backup

VRRP の Master 状態、Backup 状態で使用されるブリッジプライオリティを設定します。 **master/backup** を省略して設定した場合、両方のブリッジプライオリティに値が反映されます。

<bridge-priority>

ブリッジプライオリティ値を設定します。

デフォルト: 36864

設定範囲: 0 から 61440

その他: 値は 4096 の倍数である必要があります。

hello-time

HelloTime を設定します。

デフォルト: 2

設定範囲: 1 または 2 秒

その他: 設定値 1 はレガシーSTP で動作しているときのみ適用されます。

forward-delay

ForwardDelay を設定します。

デフォルト: 15

設定範囲: 4 から 30 秒

max-age

MaxAge を設定します。

デフォルト: 20

設定範囲: 6 から 40 秒

解説 no を指定するとデフォルト値に戻すことができます。

ssh

機能 本機器への SSH 接続のアクセスを許可します。

フォーマット [no] ssh <ipv4-net> <ipv4-mask>
[no] ssh <ipv4-net>/<ipv4-masklen>
[no] ssh <ipv6-net>/<ipv6-prefixlen>

パラメーター <ipv4-net>
SSH 接続を許可するクライアント IPv4 アドレスのネットワークアドレスを指定します。

<ipv4-mask>
<ipv4-net>に対応するネットマスクを指定します。

<ipv4-masklen>
<ipv4-net>に対応するネットマスク長を指定します。

<ipv6-net>
SSH 接続を許可するクライアント IPv6 アドレスのネットワークアドレスを指定します。

<ipv6-prefixlen>
<ipv6-net>に対応するプレフィクス長を指定します。

設定数制限:
最大 32 個の許可リストを作ることができます。

解説 工場出荷時にはすべての IPv4 アドレスからの SSH 管理アクセスが許可されていますので必要に応じて削除してください。

ssl

機能 SSL 設定モードに移動します。

フォーマット [no] ssl <ssl-name> [test]

パラメーター <ssl-name>

SSL 設定モードに移動します。該当の SSL ポリシー名が存在しない場合は SSL ポリシーを新規に作成します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

最大設定数: 256

test

テスト用の証明書が自動的にインストールされます。

ssl session-timeout

機能 SSL セッション情報の保持時間を設定します。

フォーマット [no] `ssl session-timeout` <*time-expression(hms)*>

パラメーター `session-timeout` <*time-expression(hms)*>

SSL セッション情報の保持時間を時間、分、秒単位で設定します。例えば
1h(1 時間)、30m(30 分)、2m30s(2 分 30 秒)、という表記が可能です。

デフォルト: 5 分

設定範囲: 0 秒から 24 時間

ssl3-enable

機能 SSLv3 を使用した接続を許可します。

フォーマット [no] ssl3-enable

パラメーター なし

解説 no を指定すると SSLv3 を使用した接続が禁止されます。(デフォルト動作)

sync

機能 設定情報やセッション情報の同期動作を設定します。

フォーマット [no] sync { config | session | startup-session }
sync { config | session } all

パラメーター sync config

実行したコマンドが peer に送信されます。no で実行するとコマンドが送信されなくなります。

sync session

セッション情報を Master から Backup に定期的に送信します。no で実行するとセッション情報の送信を停止します。

sync startup-session

システム起動時に既存 Master 機に対して全セッションの同期要求を送信します。

全セッションの同期は、Master 機側においても負荷分散機能の停止を伴います。

これを避けるためには no で起動時の同期を無効に設定してください。

sync session all

このコマンドを実行した瞬間の全セッション情報を Master 機と同期します。Master, Backup 機のどちらでもコマンドを実行することができます。

sync config all

すべての設定情報を同期します。

解説 sync config all を実行すると peer 側のすべての VLAN の IP アドレスは、local 側の対応する VLAN の IP アドレスの±1 が固定で設定されます。
±1 は VLAN の IP アドレスと VRRP で設定した peer-address の大小関係から自動的に算出されます。

system

機能 TCP コネクションにおける TIME_WAIT 状態の待ち時間(2MSL タイマー)を変更します。

フォーマット [no] **system msl-timer** <*time-expression (ms)*>

パラメーター <*time-expression (ms)*>

MSL タイマーを分、秒単位で設定します。例えば 1s(1 秒)、1m(1 分)、という表記が可能です。

MSL タイマーの 2 倍の値が、TIME_WAIT 状態の待ち時間(2MSL タイマー)として設定されます。

例えば、MSL タイマーを 10 秒に設定した場合、TIME_WAIT 状態の待ち時間(2MSL タイマー)は 20 秒となります。

デフォルト: 2 秒

設定範囲: 1 秒(1s)から 1 分(1m)

telnet

機能 本機器への telnet 接続のアクセスを許可します。

フォーマット [no] telnet <ipv4-net> <ipv4-mask>
[no] telnet <ipv4-net>/<ipv4-masklen>
[no] telnet <ipv6-net>/<ipv6-prefixlen>

パラメーター <ipv4-net>
telnet 接続を許可するクライアント IPv4 アドレスのネットワークアドレスを指定します。

<ipv4-mask>
<ipv4-net>に対応するネットマスクを指定します。

<ipv4-masklen>
<ipv4-net>に対応するネットマスク長を指定します。

<ipv6-net>
TELNET 接続を許可するクライアント IPv6 アドレスのネットワークアドレスを指定します。

<ipv6-prefixlen>
<ipv6-net>に対応するプレフィクス長を指定します。

設定数制限:
最大 32 個の許可リストを作ることができます。

terminal

機能 設定端末の設定を変更します。

フォーマット [no] **terminal auto-logout** <*time-expression(m)*>
[no] **terminal history-size** <*history-num*>

パラメーター **auto-logout** <*time-expression(m)*>

CLI や WebUI で許容される動作アイドル時間を分単位で設定します。

デフォルト: 10 分

設定範囲: 0 から 1440 分

その他: 0 を設定すると自動ログアウト機能が無効になります。

history-size <*history-num*>

現在のログイン時に実行したコマンドの履歴を保持する個数を設定します。

デフォルト: 100

設定範囲: 0 から 500

その他: 0 を設定するとコマンド履歴を保存しません。

解説 no を指定すると 0 を設定するのと同じ動作になります。

user-mgmt

機能 ユーザーアカウントの管理を行います。

フォーマット [no] user-mgmt <user-name> password <"password"> permission { admin | sub-admin | readonly }

パラメーター <user-name>

追加、または削除するアカウントのユーザー名を指定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)が使用可能

入力値範囲: 1 から 16 文字

その他: 先頭文字に数字、ハイフン(-)、アンダーバー(_)を使用することはできません

<password>

ログインパスワードを指定します。

入力値範囲: 1 から 32 文字

その他:

パスワード文字列に二重引用符(")、単一引用符(')、空白を含める場合は二重引用符(")で囲ってください。二重引用符(")をパスワード文字列に含める場合、バックスラッシュ(\)でエスケープしてください。パスワード文字列の末尾を空白にすることはできません。

admin

管理権限をもつユーザーアカウントを作成します。

sub-admin

管理権限をもつユーザーアカウントを作成します。ただし、当該ユーザーは WEB 管理画面の表示状態を変更する権限を持ちません。

readonly

参照権限をもつユーザーアカウントを作成します。

設定数制限:

最大 4 ユーザーまで作ることができます。

解説 自アカウントのパスワードを変更する場合には **passwd** コマンドを使用してください。

注意 既存ユーザーの権限を変更することはできません。権限を変更する場合は一度削除し、同じユーザー名で作り直す必要があります。

virtual

機能 仮想サーバー設定モードに移動します。仮想サーバーID が存在しない場合は仮想サーバーを新規に追加します。

フォーマット [no] virtual <ip-addr>.<port>.{ ftp | udp | tcp }
[no] virtual <virtual-name>

パラメーター <ip-addr>

仮想サーバーの IP アドレスを指定します。

<port>

TCP または UDP のポート番号を指定します。

0(ゼロ)は任意のポート番号を意味します。

ftp | udp | tcp

仮想サーバーのプロトコルを選択します。

FTP を負荷分散する場合は **ftp** を指定してください。

<virtual-name>

仮想サーバー設定モードの **name** コマンドで設定した名前指定することもできます。

設定数制限:

IPv4、IPv6 それぞれ最大 256 台の仮想サーバーを作ることができます。

説明 <ip-addr>、<port>、プロトコルの間にはスペースを入れることはできません。

それぞれドット「.」で区切って指定してください。

本製品では「<ip-addr>.<port>.プロトコル」で指定した文字列をサーバーIDと呼びます。

vrrp force-backup

機能 VRRP 状態を強制的に Backup に遷移させます。

フォーマット [no] vrrp force-backup

パラメーター なし

解説 no 指定で強制的な Backup 状態を解除します。

vrrp instance

機能 VRRP 設定モードに移動します。

フォーマット [no] vrrp instance <index>

パラメーター instance <index>
VRRP 設定モードに移動します。<index>には 0 を指定してください。

解説 no コマンドでインスタンスを削除することができます。

web-mgmt

機能 本機器への Web 管理アクセスを許可します。

フォーマット [no] web-mgmt <ipv4-net> <ipv4-mask>
[no] web-mgmt <ipv4-net>/<ipv4-masklen>
[no] web-mgmt <ipv6-net>/<ipv6-prefixlen>
[no] web-mgmt auto-redirect

パラメーター <ipv4-net>
Web 管理アクセスを許可するクライアント IPv4 アドレスのネットワークアドレスを指定します。

<ipv4-mask>
<ipv4-net>に対応するネットマスクを指定します。

<ipv4-masklen>
<ipv4-net>に対応するネットマスク長を指定します。

<ipv6-net> Web 管理アクセスを許可するクライアント IPv6 アドレスのネットワークアドレスを指定します。

<ipv6-prefixlen>
<ipv6-net>に対応するプレフィクス長を指定します。

auto-redirect

HTTP でのアクセスを HTTPS にリダイレクトします。デフォルト設定ではリダイレクトします。

設定数制限:
最大 32 個の許可リストを作ることができます。

解説 工場出荷時にはすべての IPv4 アドレスからの Web 管理アクセスが許可されていますので必要に応じて削除してください。

write erase

機能 設定情報を削除します。

フォーマット write erase [all | primary | secondary | current]

パラメーター all
機器の設定を工場出荷時状態に戻します。

primary | secondary | current
それぞれ primary、secondary 起動領域、現在の起動領域に保存されている設定情報を削除します。

解説 現在の起動領域は **show version** コマンドによって確認することができます。

write memory

機能 現在の設定情報をフラッシュメモリーに保存します。

フォーマット write memory

パラメーター なし

解説 コマンドの動作は `copy running-config startup-config` と同じです。

イーサネット設定モード

特権モードから interface ethernet コマンドで移行します。イーサネットポートの設定を登録・変更できます。ハイフン(-)やカンマ(,)を使用して範囲を指定することで、複数ポートの設定を変更することができます。

allowed-vlan

機 能 通過可能な VLAN ID を指定します。

フォーマット [no] allowed-vlan <vlan-id>

パラメーター <vlan-id>
受信を許可する VLAN ID を指定します。

解 説 <vlan-id>は「1,2,3」、「2-10」、「1,4-6」のように複数を同時に選択することができます。
no を指定するとデフォルトの動作に戻ります。

channel

機能 イーサネットポートを論理ポートにリンク集約します。

フォーマット [no] channel <group-num>

パラメーター <group-num>

論理チャンネルのグループ番号を指定します。

入力値範囲: イーサネットポート数により指定可能なグループ番号が異なります。

ポート数 3: 1

ポート数 6: 1 または 2

ポート数 10: 1 から 4

解説 指定したグループ番号の論理チャンネルインターフェイスが存在しない場合は自動的に生成されます。

no を指定するとリンク集約を解除します。

filter

機能 MAC アクセスフィルターをイーサネットポートに適用します。

フォーマット `filter <mac-acl-name> { in | out }`
`no filter { in | out }`

パラメーター `<mac-acl-name>`
`access-list mac` コマンドで定義した MAC アクセスリスト名を指定します。

`in, out`
それぞれ受信、送信パケットに対してフィルターが適用されます。

解説 `no` コマンドでフィルターリングを解除します。その際 `<mac-acl-name>` は指定しません。

注意 `access-list mac` コマンドでフィルターリングルールを変更した場合には、`no filter` し、再度 `filter` コマンドを実行してください。
`access-list mac` の変更だけではフィルターリングルールが更新されませんのでご注意ください。

firewall

機能 IPFW イーサネットポートリストをイーサネットポートに適用します。

フォーマット `firewall <ipfw-ethport-list-name>`
`no filter [<ipfw-ethport-list-name>]`

パラメーター `<ipfw-ethport-list-name>`
ipfw-list ethport コマンドで定義した IPFW イーサネットポートリスト名を指定します。

解説 `no` コマンドでフィルターリングを解除します。

注意 `ipfw-list ethport` コマンドで IPFW リスト内のルールを変更した場合には、`no firewall` し、再度 `firewall` コマンドを実行してください。
`ipfw-list ethport` の変更だけでは変更したルールは更新されませんのでご注意ください。

mirror-port

機能 イーサネットポートをミラーポートに設定します。

フォーマット mirror-port

パラメーター なし

解説 複数のイーサネットポートをミラーポートに設定することはできません。

monitor

機能 イーサネットポートをモニタリングし、パケットをミラーポートに転送します。

フォーマット `monitor { both | rx | tx }`

パラメーター `both`
受信、送信パケットの両方をモニタリングします。

`rx`
受信パケットのみをモニタリングします。

`tx`
送信パケットのみをモニタリングします。

解説 `mirror-port` を設定していない場合、`monitor` 設定は有効になりません。複数のイーサネットポートをモニタリングすることもできますが、データ量によってはミラー先でパケットを破棄する場合があります。

native-vlan

機能 ネイティブ VLAN を設定します。

フォーマット [no] native-vlan <vlan-id>

パラメーター <vlan-id>
ネイティブ VLAN にする VLAN の VLAN ID を指定します。

解説 802.1q タグがついていないパケットはネイティブ VLAN のパケットとして扱われます。

protected

機能 protected ポート同士の通信を禁止します。

フォーマット [no] protected

パラメーター なし

解説 同一 VLAN 内の protected ポート間でのみ通信の禁止が有効となります。

shutdown

機能 ポートを停止状態にします。

フォーマット [no] shutdown

パラメーター なし

解説 再開するには **no** を指定します。

slb

機能 イーサネットポートがどのネットワークに接続されているかを設定します。

フォーマット `slb { both | mgmt [secure] | network | server }`

パラメーター both

クライアントとサーバーの両方が接続されていることを意味します。また管理ポートとしても動作します。シングルアーム構成で接続する場合には **both** を設定してください。

mgmt

管理ポートとして動作します。管理ポートでは、受信した仮想サーバーへの ARP/NDP 問い合わせには答えません。

secure

管理専用ポートとして動作します。管理専用ポートでは、管理専用ポートへのアクセスや、管理専用ポートを経由するアクセスを制限します。

network

クライアントが接続されているものとして動作します。

server

サーバーが接続されているものとして動作します。

解説 本設定はフェイルスルー設定時には必須の設定となりますが、非フェイルスルー設定時にでも使用することができます。

注意 フェイルスルー設定時には、ポート 1 が **network**、ポート 2 が **server** に設定されます。
フェイルスルー設定を解除した場合でも自動的に設定された **slb** コマンドでのポート属性の設定は保持されますのでご注意ください。

spanning-tree

機能 イーサネットポートや論理チャンネルに反映されるスパニングツリーの設定を行います。

フォーマット [no] spanning-tree
[no] spanning-tree edge
[no] spanning-tree priority <port-priority>
[no] spanning-tree cost <port-cost>
spanning-tree restart

パラメーター [no] spanning-tree
スパニングツリーを開始します。停止する場合は **no** コマンドで停止します。

edge

このポートを edge ポートに設定します。 **no** で設定を解除します。

priority <port-priority>

ポートプライオリティを設定します。

cost <port-cost>

ポートコストを設定します。

restart

802.1D 互換モードで動作中のポートを強制的に RSTP で再開します。

speed

機能 イーサネットポートのリンク速度を変更します。

フォーマット speed { 10half | 10full | 100half | 100full | 1000full | auto }

パラメーター 10, 100, 1000
それぞれリンク速度を意味します。

half, full
それぞれ伝送方式が半二重、全二重を意味します。

auto
リンク速度、伝送方式ともにオートネゴシエーションで動作します。

tagged

機能 タグ VLAN を有効にします。

フォーマット [no] tagged

パラメーター なし

解説 デフォルトでは **interface vlan** で設定されているすべての VLAN のパケットを受け入れます。
処理する VLAN のパケットは、必要に応じて **allowed-vlan** コマンドで制限してください。
no を指定するとタグ付を解除します。

vlan

機能 ポートが所属する VLAN を設定します。

フォーマット vlan <vlan-id>

パラメーター <vlan-id>
VLAN ID を指定します。

チャンネル設定モード

特権モードから `interface channel` コマンドで移行します。チャンネルインターフェイスの設定を登録・変更できます。イーサネット設定モードとは違い、複数のチャンネル番号を指定することはできません。

`allowed-vlan`
`firewall`
`native-vlan`
`protected`
`slb`
`spanning-tree`
`tagged`
`vlan`

解 説 これらのコマンドについては `interface ethernet` モードの説明をご参照ください。

mode

機能 リンク集約の動作モードを変更します。

フォーマット `mode { lacp | static }`

パラメーター `lacp`
LACP によるネゴシエーションを行います。

static
LACP を使用しません。

VLAN 設定モード

特権モードから `interface vlan` コマンドで移行します。VLAN の設定を登録・変更できます。

filter

機能 IPv4, IPv6 アクセスフィルターを VLAN インターフェイスに適用します。

フォーマット `filter { ipv4 | ipv6 } <ip-acl-name>`
`no filter { ipv4 | ipv6 }`

パラメーター `ipv4 <ip-acl-name>`
`access-list ip` コマンドで定義したアクセスリスト名を指定します。

`ipv6 <ip-acl-name>`
`access-list ipv6` コマンドで定義したアクセスリスト名を指定します。

解説 `no` コマンドでフィルターリングを解除します。その際 `<ip-acl-name>` は指定しません。

注意 `access-list ipv[46]` コマンドでフィルターリングルールを変更したい場合には、`no filter` し、再度 `filter` コマンドを実行してください。
`access-list ipv[46]` の変更だけではフィルターリングルールが更新されませんのでご注意ください。

firewall

機能 IPFW VLAN リストを VLAN インターフェースに適用します。

フォーマット `firewall <ipfw-vlan-list-name>`
`no filter [<ipfw-vlan-list-name>]`

パラメーター `<ipfw-vlan-list-name>`
`ipfw-list vlan` コマンドで定義した IPFW VLAN リスト名を指定します。

解説 `no` コマンドでフィルターリングを解除します。

注意 `ipfw-list vlan` コマンドで IPFW リスト内のルールを変更した場合には、`no firewall` し、再度 `firewall` コマンドを実行してください。
`ipfw-list vlan` の変更だけでは変更したルールは更新されませんのでご注意ください。

ip address

機能 VLAN インターフェイスに IP アドレスを設定します。

フォーマット [no] ip address <ipv4-addr> [<ipv4-mask>]
[no] ip address <ipv4-addr>/<masklen>
[no] ip address <ipv6-addr>/<prefixlen>

パラメーター <ipvX-addr>
IPvX アドレスを設定します。

<ipv4-mask>
IPv4 アドレスのサブネットマスクを指定します。

</masklen>
IPv4 アドレスのサブネットマスク長を/「スラッシュ」区切りで指定します。

</prefixlen>
IPv6 アドレスのプレフィクス長を/「スラッシュ」区切りで指定します。

ip redundant-address

機能 VLAN インターフェイスに冗長 IP アドレスを設定します。

フォーマット [no] ip redundant-address <ip-addr>

パラメーター <ip-addr>
IPv4 または IPv6 アドレスを設定します。

解説 **redundant-address** は IPv4、IPv6 アドレスを一つずつ設定することができます。
redundant-address は冗長構成で Master 状態になったときにのみ有効になります。

ip virtual-address

機能 VLAN インターフェイスに仮想 IP アドレスを設定します。

フォーマット [no] ip virtual-address <ip-addr>

パラメーター <ip-addr>
IPv4 または IPv6 アドレスを設定します。

解説 **virtual** コマンドで仮想サーバーを定義する前に **ip virtual-address** で仮想 IP アドレスを定義する必要があります。
仮想 IP アドレスは **virtual** コマンドで **enable** 状態になるまで ARP や NDP に応答しません。

mtu

機能 VLAN の MTU 値を設定します。

フォーマット `mtu <mtu-size>`

パラメーター `<mtu-size>`

VLAN に IPv6 アドレスが設定されている場合、最小の MTU は 1280 バイトになります。

入力値範囲: 576 から 1500

解説 機器に tagged ポートが設定されている場合、全ての VLAN の MTU 値が `<mtu-size>` で指定した MTU 値に統一されます。

注意 MTU を小さい値から大きな値に変更する場合は機器の再起動が必要になります。

name

機能 VLAN 名を設定します。

フォーマット [no] name <vlan-name>

パラメーター <vlan-name>

各 VLAN の識別用に VLAN 名を設定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

route-id

機能 VLAN で使用するルーティングテーブルのルート ID を設定します。

フォーマット [no] route-id <num>

パラメーター <num>
ルート ID を指定します。
入力値範囲: 0 から 15

rtadv

機能 ルーター広告の設定を行います。

フォーマット [no] rtadv [flag { managed | other | both }] [dns primary <ipv6-addr> [secondary <ipv6-addr>]]

パラメーター managed | other | both
それぞれ RA の M フラグ、O フラグ、両方のフラグがセットされます。

dns primary <ipv6-addr>, secondary <ipv6-addr>
ルーター広告の DNS オプションを有効にします。

vlan-mac

機能 VLAN インターフェイスが使用する MAC アドレスを変更します。

フォーマット `vlan-mac <port-num>`

パラメーター `<port-num>`
変更したい MAC アドレスを持つイーサネットポート番号を指定します。

解説 初期値はイーサネットポート 1 の MAC アドレスが使用されます。
初期値に戻す場合は `<port-num>` に「1」を指定してください。

vrrp backup-l2forward

機能 冗長構成の Backup 状態のときに L2 フォワーディングを許可します。

フォーマット [no] vrrp backup-l2forward

パラメーター なし

解説 no で Backup 状態時に L2 フォワーディングを停止させることができます。

vrrp vrid

機能 冗長構成の VRRP 広告で使用する仮想ルーターID を設定します。

フォーマット [no] vrrp vrid <vrid>

パラメーター <vrid>
仮想ルーターID を指定します。
入力値範囲: 1 から 255

解説 仮想ルーターID は同じネットワーク内の他の機器と重複しないように選択してください。

NAT プール設定モード

特権モードから `nat-pool` コマンドで移行します。本機器の NAT 処理で使用するためのアドレスプールを登録・変更できます。

ip address

機能 NAT プールに IP アドレスを追加します。

フォーマット [no] ip address <ipv4-addr>
[no] ip address range <ipv4-addr-start> <ipv4-addr-end>
[no] ip address <ipv6-addr>
[no] ip address range <ipv6-addr-start> <ipv6-addr-end>

パラメーター <ipvX-addr>
NAT プールに IP アドレスを一つ追加します。

<ipvX-addr-start>
IP アドレスを範囲指定して追加する際の開始 IP アドレスを指定します。

<ipvX-addr-end>
IP アドレスを範囲指定して追加する際の終端 IP アドレスを指定します。

設定数制限:
NAT プールにはシステム全体で最大 16 個まで IP アドレスを設定することができます。

解説 NAT プールアドレスには `interface vlan` モードの `ip virtual-address` コマンドで設定した仮想 IP アドレスを含めることができます。
仮想 IP アドレスをプールアドレスに設定する場合は、上記 16 個の設定数制限には含まれません。

リバース NAT 設定モード

特権モードから `reverse-nat` コマンドで移行します。サーバーから発信されるパケットに対する NAT 処理の設定を登録・変更できます。

bind

機能 リバース NAT プールに実サーバーを割り当てます。

フォーマット `[no] bind <ip-addr>.<port> [dstport <port>]`

パラメーター `<ip-addr>`

リバース NAT したいサーバーの IP アドレスを設定します。

`<port>`

リバース NAT したいサーバーの送信元ポートを設定します。

dstport `<port>`

特定の宛先ポートのみを NAT する場合に指定してください。

デフォルトでは任意の宛先ポートに対しての接続をアドレス変換します。

解説 `<ip-addr>.<port>` で指定された IP アドレスとポート番号を持つパケットが NAT されます。

enable

機能 リバース NAT エントリーを有効化します。

フォーマット [no] enable

パラメーター なし

ftp-data-port

機能 ftp モードのとき PORT 接続の ftp サーバー側ポート番号を変更したいときに指定します。
指定なし(デフォルト)のとき、制御コネクト -1 のポートが自動時に使用されます。

フォーマット [no] ftp-data-port [port-num]

パラメーター port-num
ポート番号 1~65535 を指定します。

route-id

機能 リバース NAT で使用するルーティングテーブルのルート ID を設定します。

フォーマット [no] route-id <num>

パラメーター <num>
ルート ID を指定します。
入力値範囲: 0 から 15

timeout

機能 リバース NAT セッションのアイドルタイムアウトを設定します。

フォーマット `timeout <time-expression (dhms)>`

パラメーター `<time-expression (dhms)>`

生存時間を日、時間、分、秒分単位で設定します。

デフォルト: TCP 30 分, UDP 5 分

設定範囲: 1 秒(1s)から 365 日(365d)。

SSL 設定モード

特権モードから `ssl` コマンドで移行します。SSL アクセラレーションで使用するための SSL 証明書ポリシーを登録します。

`crl`

機能 クライアント証明書の失効状態を確認するための CRL を定期的に取得する設定です。

フォーマット `[no] crl <url> [interval <time-expression(dhm)>]`

パラメーター `<url>`

http または https で始まる URL を指定します。

`<url>`内に IPv6 アドレスを記述する場合、角括弧「`[]`」の間に記述してください。

interval `<time-expression(dhm)>`

CRL の更新間隔を日、時間、分単位で設定します。例えば 1h(1 時間)、30m(30 分)、2h50m(2 時間 50 分)、1d(1 日)、という表記が可能です。

デフォルト: 60 分

設定範囲: 1 分(1m)から 365 日(365d)

解説 プロキシサーバーを経由する必要がある場合は別途 `proxy` コマンドで設定してください。

csr

機能 電子証明書署名要求(CSR)を生成します。

フォーマット csr

パラメーター なし

VRRP 設定モード

特権モードから `vrrp instance 0` コマンドで移行します。VRRP プライオリティなどの設定値を登録・変更できます。第二引数は省略可能ですが、指定する場合必ず 0 を指定します。

delay

機能 Backup 状態に遷移してから VRRP 広告を受信するまでの遅延時間を設定します。

フォーマット `[no] delay <time-expression(s)>`

パラメーター `<time-expression(s)>`
遅延時間を設定します。
デフォルト: 遅延なし
設定範囲: 0 秒から 100 秒

interval

機能 VRRP 広告の送信インターバルを設定します。

フォーマット [no] interval <interval>

パラメーター <interval>

インターバルを 10msec 単位で設定します。

デフォルト: 100 (=1 秒)

設定範囲: 1 から 4095

解説 Backup から Master 状態への遷移時間は、送信インターバルの約 3 倍の時間になります。

遷移時間の最小値は 200ms です。

<interval>に 1 から 6 を設定した場合でも遷移時間は 200ms となります。

ip peer-address

機能 冗長構成を組む相手の IP アドレスを設定します。

フォーマット [no] peer-address <ip-addr>

パラメーター <ip-addr>
IPv4 または IPv6 アドレスを設定します。

preempt

機能 preempt を有効にすると、VRRP プライオリティーの値によって Master、Backup を決定します。

フォーマット [no] preempt

パラメーター なし

解説 preempt が無効の場合は、ネットワークに先に存在していた機器が Master になります。

priority

機能 VRRP プライオリティーを設定します。

フォーマット `priority <priority> [peer <priority>]`

パラメーター `<priority>`

VRRP プライオリティーを設定します。

デフォルト: 100

設定範囲: 1 から 254

peer <priority>

冗長相手機器の VRRP プライオリティーを変更することができます。

省略した場合、本機器と相手機器の両方に第一引数の `<priority>` が設定されます。

設定範囲: 1 から 254

解説 `preempt` が有効の場合、VRRP プライオリティーの大きい機器が Master に選出されます。

track

機能 イーサネットポートのリンクを監視し、VRRP 状態に反映させます。リンクの監視結果を VRRP プライオリティーに反映させることもできます。

フォーマット [no] track group <group-num> ethernet <port-num-expression>
[decrement <value>]

パラメーター group <group-num>
グループ番号を指定します。設定範囲: 1 から 12

ethernet <port-num-expression>
グループ化するイーサネットポートのポート番号を指定します。カンマ「,」
やハイフン「-」で複数のポートを同時に指定することができます。

decrement <value>
VRRP プライオリティーの減算値を指定します。各ポートがリンクダウンする
たびに減算が行われます。省略した場合は減算を行いません。
設定範囲: 1 から 253

解説 同一グループのイーサネットポートがすべてリンクダウンすると Master 機は
VRRP 広告の送信を停止します。

ヘルスチェック設定モード

特権モードから probe コマンドで移行します。サーバーに対するヘルスチェック設定を登録・変更できます。

dns

機能 DNS のサーバーヘルスチェックを行います。

フォーマット `dns <host-name> { A | AAAA }`
`[no] dns`

パラメーター `<host-name>`
名前解決をしたいホスト名を指定します。

A, AAAA
DNS クエリの種別を指定します。

解説 DNS のサーバーヘルスチェックは、TCP または UDP のヘルスチェック時に設定が可能です。

enable

機能 ヘルスチェックを有効化します。

フォーマット [no] enable

パラメーター なし

ftp

機能 FTP のサーバーヘルスチェックを行います。

フォーマット [no] ftp

パラメーター なし

解説 FTP のサーバーヘルスチェックは、TCP のヘルスチェック時に設定が可能です。

http

機能 HTTP のサーバーヘルスチェックを行います。

フォーマット `http <"request"> { status <status-code> ... | string <"response"> }`
`[no] http`

パラメーター `<"request">`

HTTP のリクエスト文字列を指定します。リクエスト文字列はダブルクォート「"」で囲ってください。

status `<status-code> ...`

ヘルスチェックが ALIVE となる HTTP ステータスコードを設定します。

`<status-code>`は空白区切りで 4 つまで指定することができます。

それぞれ範囲指定することが可能で、「200-299」、「100 200-299 304」のように指定します。

string `<"response">`

ヘルスチェックが ALIVE となる HTTP の応答文字列を設定します。応答文字列はダブルクォート「"」で囲ってください。

解説 HTTP のサーバーヘルスチェックは、TCP のヘルスチェック時に設定が可能です。

imap4

機能 IMAP4 のサーバーヘルスチェックを行います。

フォーマット [no] imap4

パラメーター なし

解説 IMAP4 のサーバーヘルスチェックは、TCP のヘルスチェック時に設定が可能です。

interval

機能 ヘルスチェックを行う間隔を設定します。

フォーマット [no] interval <time-expression(s)>

パラメーター <time-expression(s)>

ヘルスチェックを行う間隔を秒単位で設定します。

デフォルト: 5 秒

設定範囲: 1 から 255 秒

解説 サーバーからの応答を待ち受けるタイプのヘルスチェックの場合、intervalの間隔がなければヘルスチェックエラーと判断されます。

manual-failback

機能 実サーバーが DOWN から ALIVE に変化したときの復旧動作を変更します。

フォーマット [no] manual-failback

パラメーター なし

注意 **manual-failback** を設定したヘルスチェックエントリーで実サーバーが DOWN と判定されると 該当の実サーバーは自動的に **no enable** 状態に変化し、ALIVE 状態になっても負荷分散対象になりません。実サーバーを再度負荷分散対象に加えるためには **enable real** コマンドで実サーバーを有効状態に設定してください。

ntp

機能 NTP のサーバーヘルスチェックを行います。

フォーマット [no] ntp

パラメーター なし

解説 NTP のサーバーヘルスチェックは、UDP のヘルスチェック時に設定が可能です。

persist

機能 HTTP ヘルスチェックでキープアライブを有効にします。

フォーマット [no] persist

パラメーター なし

解説 **persist** を有効にすると HTTP ヘルスチェックで接続を維持しようとします。
デフォルトの **no persist** 状態ではヘルスチェックの試行毎に接続を確立しなおします。

pop3

機能 POP3 のサーバーヘルスチェックを行います。

フォーマット [no] pop3

パラメーター なし

解説 POP3 のサーバーヘルスチェックは、TCP のヘルスチェック時に設定が可能です。

retry

機能 ヘルスチェックの再試行回数を設定します。

フォーマット [no] **retry** <retry-times>

パラメーター <retry-times>

ヘルスチェックの再試行回数を設定します。

デフォルト: 2

設定範囲: 0 から 255

解説 ヘルスチェックが失敗すると **retry** 回数だけ再試行します。連続して失敗するとサーバーDOWN と判断されます。

smtp

機能 SMTP のサーバーヘルスチェックを行います。

フォーマット [no] smtp

パラメーター なし

解説 SMTP のサーバーヘルスチェックは、TCP のヘルスチェック時に設定が可能です。

仮想サーバー設定モード

特権モードから `virtual` コマンドで移行します。仮想サーバー設定を登録・変更できます。

access-log

機能

フォーマット [no] `access-log` <ip-addr> <facility.level>

パラメーター <ip-addr>

SYSLOG サーバーの IP アドレスを指定します。

<facility.level>

facility: ログファシリティを設定します。

デフォルト: 20 (=LOCAL4)

設定範囲: 16 から 23。数字はそれぞれ LOCAL0 から LOCAL7 を意味します。

level: ログレベルを設定します。数字が小さいほど重大なログであることを意味します。

デフォルト: 5 (=Notice)

設定範囲: 0 から 7。

解説 `access-log` は仮想サーバー毎に設定することができます。 `logging` コマンドの設定状態とは関連していません。

authfail

機能 クライアント認証が失敗したときの動作を設定します。

フォーマット [no] authfail { alert | forbid | redirect <url> }

パラメーター alert
SSLのアラートを返信します。

forbid
HTTPのステータスコード 403 を返信します。

redirect
HTTPのステータスコード 302 を返信し、他の URL へリダイレクトします。

解説 **no authfail** コマンドを実行するとクライアント認証が失敗したときでも通常のSSLアクセラレーションを行います。

backup-policy

機能 バックアップサーバー、またはオーバーフローサーバーを起動するタイミングを設定します。

フォーマット `backup-policy { single | multi } [failback { forced | orderly }]`

パラメーター [バックアップサーバーの動作]

single

すべてのプライマリサーバーが DOWN したときにバックアップサーバーが一台起動します。

multi

プライマリサーバーが一台 DOWN するごとに、一台のバックアップサーバーを起動します。

[オーバーフローサーバーの動作]

single

すべてのプライマリサーバーが最大コネクションに達したときにオーバーフローサーバーが一台起動します。

multi

プライマリサーバーが最大コネクションに達するごとに、一台のオーバーフローサーバーを起動します。

[共通の動作]

forced

プライマリサーバーが起動しフェイルバックした際に、待機系サーバーへのセッション維持情報 (sticky 情報) の使用を止め、接続を強制的にプライマリサーバーに戻します。

orderly

プライマリサーバーが復帰して、フェイルバック動作が発生しても、現在生成されている待機系サーバーへのセッション維持情報 (sticky 情報) を使用し、ゆるやかに接続をプライマリサーバーに戻します。

解説 待機系のサーバーとはバックアップサーバー、またはオーバーフローサーバーに設定された実サーバーを指します。
本ページでは `bind` コマンドで `backup/overflow` が指定されていない通常のサーバーのことをプライマリサーバーと呼称しています。

bind

機能 仮想サーバーの配下に置く実サーバーやソーリーコンテンツを指定します。

フォーマット [no] bind <ip-addr>.<port> [group <group-id>] [weight <weight-value>]
[dsr] [backup] [overflow] [maxconns <connection-num>]

[no] bind content <content-name>

パラメーター <ip-addr>.<port>

仮想サーバーの配下に置かれる実サーバーの ID を指定します。

group <group-id>

ソース IP アドレス負荷分散や L7 スイッチングの機能を使用する場合、分散先のグループ ID を指定します。

設定範囲: 1 から 31

weight <weight-value>

この実サーバーの重みを設定します。

デフォルト: 1

設定範囲: 0 から 255

dsr

この実サーバーが DSR 動作を行う場合、本オプションを指定します。

backup

この実サーバーをバックアップサーバーにする場合、本オプションを指定します。

プライマリーサーバーが DOWN したときに負荷分散対象となるサーバーです。

overflow

この実サーバーをオーバーフローサーバーにする場合、本オプションを指定します。

プライマリーサーバーが最大コネクションに達したときに負荷分散対象となるサーバーです。

maxconns <connection-num>

確立できるコネクションの最大値を指定します。

デフォルト: 無制限(0)

設定範囲: 0 から 65535

content <content-name>

全ての実サーバーが DOWN したときに表示するソーリーコンテンツを指定し

ます。

`<content-name>`は **import content** でコンテンツファイルをインポートしたときに指定したコンテンツ名を使用します。

解説 `<ip-addr>.<port>`についてはあらかじめ **real** コマンドで設定されている必要があります。
ソーリーコンテンツ機能と `fallback-url` 機能が同時に設定されている場合は、`fallback-url` の設定が優先されます。

certhead

機能 クライアント認証で使した証明書を HTTP ヘッダーに挿入します。

フォーマット [no] certhead <header-name> [base64 | pem]

パラメーター <header-name>

HTTP ヘッダーに埋め込む際のヘッダー名をここで指定します。
入力値範囲: 1 から 16 文字

base64

base64 形式に変換したクライアント証明書を挿入します。
省略した場合、base64 形式が選択されます。

pem

pem 形式に変換したクライアント証明書を挿入します。

解説 ヘッダー名を client-cert にした場合、「client-cert: ~」のような HTTP ヘッダーが既存ヘッダー内に挿入されます

cipher-suite

機能 SSL アクセラレーションで使用する暗号スイートを指定します。

フォーマット [no] cipher-suite <"cipher-expression">

パラメーター <"cipher-expression">

暗号スイート名を二重引用符内に複数記載して設定します。暗号スイートは以下のものが使用可能です。

DES-CBC-SHA, DES-CBC3-SHA, AES128-SHA, AES128-SHA256, AES256-SHA, AES256-SHA256, AES128-GCM-SHA256, AES256-GCM-SHA384, DHE-AES128-SHA, DHE-AES128-SHA256, DHE-AES128-GCM-SHA256, DHE-AES256-SHA, DHE-AES256-SHA256, DHE-AES256-GCM-SHA384, ECDHE-RSA-AES128-SHA, ECDHE-RSA-AES128-SHA256, ECDHE-RSA-AES128-GCM-SHA256, ECDHE-RSA-AES256-SHA, ECDHE-RSA-AES256-SHA384, ECDHE-RSA-AES256-GCM-SHA384, ECDHE-ECDSA-AES128-SHA, ECDHE-ECDSA-AES128-SHA256, ECDHE-ECDSA-AES128-GCM-SHA256, ECDHE-ECDSA-AES256-SHA, ECDHE-ECDSA-AES256-SHA384, ECDHE-ECDSA-AES256-GCM-SHA384

いくつかの暗号スイートをまとめた抽象表記も可能です。下記の表記が使用可能です。

ALL, DES, DES3, RC4, AES, AES128, AES256, SHA, SHA256, SHA384, DHE, GCM, CBC, ECDHE, ECDSA

カンマ(,)で暗号スイート文字列、もしくは抽象表記を繋げます。空白は使用できません。

解説 デフォルトでは DES-CBC-SHA と ECDHE 系の暗号スイートは無効となります。

enable

機能 仮想サーバーを有効化します。

フォーマット [no] enable

パラメーター なし

解説 no を指定すると仮想サーバーが無効化されます。仮想サーバーは無効がデフォルトになります。
特権モードにおいては、仮想サーバーID を指定する **enable virtual** コマンドも使用することができます。

fallback-url

機能 全ての実サーバーへの接続ができなくなった場合にリダイレクトする URL を設定します。

フォーマット [no] **fallback-url** <url>

パラメーター http または https で始まる URL を指定します。
<url>内に IPv6 アドレスを記述する場合、角括弧「[]」の間に記述してください。

解説 ソーリーコンテンツ機能と fallback-url 機能が同時に設定されている場合は、fallback-url の設定が優先されます。

ftp-data-port

機能 ftp モードのとき PORT 接続のサーバー側ポート番号を変更したいときに指定します。
指定なし(デフォルト)のとき、制御コネクト -1 のポートが自動時に使用されます。

フォーマット [no] ftp-data-port [port-num]

パラメーター port-num
ポート番号 1~65535 を指定します。

header

機能 HTTP ヘッダーを挿入します。

フォーマット [no] header insert { x-forwarded-for | x-forwarded-proto | both }

パラメーター **x-forwarded-for**

「X-Forwarded-For」ヘッダーを HTTP ヘッダーに追加します。ヘッダーにはソース IP アドレスがセットされます。

x-forwarded-proto

「X-Forwarded-Proto」ヘッダーを HTTP ヘッダーに追加します。ヘッダーには http または https がセットされます。

both

「X-Forwarded-For」「X-Forwarded-Proto」の両方を追加します。

match

機能 ソース IP アドレスルールと L7 スイッチングルールにグループ ID を割り当てます。

フォーマット [no] match { <ipv4-addr> [<ipv4-mask>] | <ipv4-addr>/<masklen> | <ipv6-addr>/<prefixlen> } group <group-id>
[no] match { <rule-name> | default } { group <group-id> | redirect <scheme> <domain> <path> [<port>] | forbid }

パラメーター <ipvX-addr>

グループ化するソース IPvX アドレスを設定します。

<ipv4-mask>

IPv4 アドレスのサブネットマスクを指定します。

<masklen>

IPv4 アドレスのサブネットマスク長を/「スラッシュ」区切りで指定します。

<prefixlen>

IPv6 アドレスのプレフィクス長を/「スラッシュ」区切りで指定します。

group <group-id>

グループ ID を割り当てます。

設定範囲: 1 から 31

<rule-name>

rule コマンドで作成した L7 スイッチングルール名を指定します。

default

全ての L7 スイッチングルールにマッチしなかった場合に適用されるルールです。

redirect

ルールにマッチしたリクエストに対してリダイレクト(ステータスコード 302)で応答します。

<scheme>

リダイレクト先のスキームを指定します。http または https が設定できます。

<domain>

リダイレクト先のドメイン名を指定します。例. 「www.example.com」など。IPv6 アドレスを使用する場合は大括弧「[]」で囲う必要があります。

<path>

リダイレクト先のパスを指定します。例. 「/sales/index.php」

<port>

*<scheme>*が http で 80 以外のポート。https で 443 以外のポートにリダイレクトする場合に指定します。

forbid

ルールにマッチしたリクエストに対して Forbidden(ステータスコード 403)で応答します。

設定数制限:

IP スイッチングルールは、ひとつのグループ ID に対して最大 256 のサブネットを設定することができます。

L7 スイッチングルールは仮想サーバーあたり最大 32 個のルールを設定することができます。

name

機能 仮想サーバー名を設定します。

フォーマット [no] name <virtual-server-name>

パラメーター <virtual-server-name>

仮想サーバー名を設定します。

入力値制限: 半角英数、ハイフン(-)、アンダーバー(_)、シャープ(#)、スラッシュ(/)、コマーシャルアット(@)が使用可能

入力値範囲: 1 から 64 文字

その他: 先頭文字に数字、記号を使用することはできません

解説 特権モードの **name** コマンドとは違い、仮想サーバーID に対して名前を設定します。

onearm-gateway-mode

機能 ワンアーム構成時の動作モードを設定します。

フォーマット [no] onearm-gateway-mode

パラメーター なし

解説 ワンアーム構成でソース NAT 設定を使用せずに負荷分散を行います。
no を指定すると設定が削除されます。
仮想サーバーと同じネットワークアドレスからアクセスする場合にはソース NAT を行う必要があります。

permit-nat-filter

機能 ソース NAT フィルター設定を実施して、指定したネットワークアドレスからのアクセスにのみ、送信元アドレス変換機能(**source-nat**)を適用します。

フォーマット [**no**] **permit-nat-filter** { <ipv4-addr> <ipv4-mask> | <ipv4-addr>/<masklen> | <ipv6-addr>/<prefixlen> }

パラメーター <ipvX-addr>

送信元アドレス変換機能を適用するソース IPvX アドレスを設定します。

<ipv4-mask>

IPv4 アドレスのサブネットマスクを指定します。

<masklen>

IPv4 アドレスのサブネットマスク長を/「スラッシュ」区切りで指定します。

<prefixlen>

IPv6 アドレスのプレフィクス長を/「スラッシュ」区切りで指定します。

設定数制限:

ソース NAT フィルター設定は、ひとつの仮想サーバーに対して最大 256 のサブネットを設定することができます。

解説 ソース NAT フィルター設定を実施するには、**source-nat** コマンドが設定されている必要があります。
no source-nat コマンドにより、仮想サーバーのソース NAT 機能が無効に設定された場合、該当の仮想サーバーに設定された全てのソース NAT フィルター設定が自動で削除されます。

predictor

機能 仮想サーバーにバインドしている実サーバーへの接続の割り当てポリシーを指定します。

フォーマット `predictor { load | robin }`

パラメーター `load`

接続中の接続数が最も少ないサーバーへ割り当てます。

`robin`

バインドされた実サーバーに順番に接続を割り当てます。

解説 `load` 設定時、接続中の接続数が等しい場合は累積の接続数が一番少ないサーバーに接続を割り当てます。

route-id

機能 仮想サーバーで使用するルーティングテーブルのルート ID を設定します。

フォーマット [no] route-id <num>

パラメーター <num>
ルート ID を指定します。
入力値範囲: 0 から 15

sidheader

機能 クライアント認証を行った際の SSL セッション ID を HTTP ヘッダーに挿入します。

フォーマット [no] **sidheader** <header-name>

パラメーター <header-name>
HTTP ヘッダーに埋め込む際のヘッダー名をここで指定します。
入力値範囲: 1 から 16 文字

解説 ヘッダー名を ssl-session-id にした場合、「ssl-session-id: XXXX」のような HTTP ヘッダーが既存ヘッダー内に挿入されます

source-nat

機能 ソース NAT を設定します。

フォーマット [no] source-nat <natpool-name>

パラメーター <natpool-name>
NAT に使用するプールアドレス名を指定します。

解説 <natpool-name>はあらかじめ **nat-pool** コマンドで定義したものを使用します。

ssl

機能 仮想サーバーに SSL ポリシーを関連付けます。

フォーマット [no] ssl <ssl-name> [default]

パラメーター <ssl-name>

特権モードの **ssl** コマンドで定義した SSL ポリシー名を指定します。

default

このオプションを指定した SSL ポリシーは SNI におけるデフォルトポリシーとして使用されます。

設定数制限:

仮想サーバーに対しては最大 32 個の SSL ポリシーを設定することができます。

sticky

機能 複数のセッションを同一のサーバーに割り当てるセッション維持設定を行います。

フォーマット [no] sticky { { generic | x-forwarded-for } [mask <mask-len>] | ssl | cookie <cookie-name> [insert { always | once }] } [timeout <time-expression (dhm)>]

パラメーター generic

IP ヘッダーのソース IP アドレス情報を基に、IP アドレスが同じセッションを同じ実サーバーに割り当てます。

x-forwarded-for

HTTP リクエストの X-Forwarded-For ヘッダーから読み取った IP アドレス情報を基に、IP アドレスが同じセッションを同じ実サーバーに割り当てます。

mask <mask-len>

IP アドレス単位ではなくサブネットマスク単位でセッションを維持したい場合、**generic** あるいは **x-forwarded-for** オプションに **mask** を指定し、任意のマスク/プレフィックス長を入力します。

入力値範囲: IPv4 仮想サーバー=1 から 32, IPv6 仮想サーバー=1 から 128

ssl

SSL セッション ID が同じ接続を同じ実サーバーに割り当てます。

cookie <cookie-name>

<cookie-name>には HTTP の Cookie ヘッダーの NAME パラメーターを指定します。NAME の値が同じ接続を、同じ実サーバーに割り当てます。

入力値範囲: 1 から 255 文字

入力値制限: 以下の記号を含めることはできません。

() < > @ , ; \ " / [] ? = { } SP HT

※SP : 半角スペース、 HT : 水平タブ

insert

サーバーが発行した Cookie を使用せず、Netwiser が Cookie を発行します。

always

サーバーからの全ての HTTP 応答に Cookie を挿入します。

once

HTTP リクエストに該当の Cookie が含まれていない場合のみ Cookie を挿入します。

timeout <*time-expression (dhm)*>

セッション維持の有効時間を日、時、分単位で設定します。例えば 1 分 (1m)、1 時間(1h)、1 日(1d)、1 日と 1 時間 1 分(1d1h1m)、という表記が可能です。

デフォルト: generic と ssl は 15 分。cookie は 30 分。insert オプション付き cookie は 0 秒(クライアントのブラウザが閉じられるまで有効)。

入力値範囲: insert オプション付き cookie は 0 分(0m)から 365 日(365d)。その他は 1 分(1m)から 365 日(365d)。

timeout

機能 Layer4 セッションのアイドルタイムアウトを設定します。

フォーマット [no] timeout <time-expression (dhms)>

パラメーター <time-expression (dhms)>

生存時間を日、時間、分、秒単位で設定します。例えば 1h(1 時間)、30m(30 分)、2m30s(2 分 30 秒)、という表記が可能です。

0(または 0s)は無制限を意味します。ただし、udp 仮想サーバーには、0 (または 0s) を指定しないでください。

デフォルト: TCP 30 分, UDP 5 分

設定範囲: 0 秒(0s)から 365 日(365d)

xff-balancing

機能 X-Forwarded-For スイッチング機能を有効にして、X-Forwarded-For ヘッダーから読み取った IP アドレス情報を基に IP スイッチングを行います。

フォーマット [no] xff-balancing

パラメーター なし

解説 no を指定すると X-Forwarded-For スイッチングが無効化されます。無効状態がデフォルトです。
X-Forwarded-For スイッチング機能を有効にするには IP スイッチングルールが登録済みである必要があります。
また、本設定が有効であっても、全ての IP スイッチングルールが削除された場合、自動で無効化されます。

IP アクセスリスト設定モード

特権モードから `access-list ipv4` コマンドで移行します。VLAN インターフェイスに対してパケットの許可・拒否を行うための、IP アクセスリストを登録・変更できます。

deny

機能 IPv4 アクセスリストに拒否ルールを追加します。

フォーマット `[line <line-num>]`

`deny <proto> <src-addr> <dst-addr> [log]`

`deny { tcp | udp } <src-addr> [<src-por>] <dst-addr> [<dst-port>] [log]`

`deny icmp <src-addr> <dst-addr> [type <icmp-type>] [log]`

`no line <line-num>`

パラメーター `line <line-num>`

ルールの行番号を指定します。アクセスリストは若い番号のルールから評価されます。

`<proto>`

プロトコル番号またはプロトコル名を指定します。

`tcp` または `udp` の場合は `<src-por>`、`<src-por>` を指定することができます。

`icmp` の場合は `<icmp-type>` を指定することができます。

`<src-addr>`

送信元 IP アドレスを指定します。`any` を指定した場合は全ての IP アドレスにマッチします。

`<src-por>`

送信元ポート番号を指定します。

`<dst-addr>`

宛先 IP アドレスを指定します。`any` を指定した場合は全ての IP アドレスにマッチします。

`<dst-port>`

宛先ポート番号を指定します。

`type <icmp-type>`

ICMP タイプを指定します。

`log`

ルールにマッチしたときにログを出力します。

permit

機能 IPv4 アクセスリストに許可ルールを追加します。

フォーマット [`line` *<line-num>*]

`permit` *<proto>* *<src-addr>* *<dst-addr>*

`permit` { `tcp` | `udp` } *<src-addr>* [*<src-port>*] *<dst-addr>* [*<dst-port>*]

`permit icmp` *<src-addr>* *<dst-addr>* [`type` *<icmp-type>*]

`no line` *<line-num>*

パラメーター 設定パラメーターについては `deny` コマンドを参照してください。

解説 `permit` コマンドでは `log` オプションを指定することはできません。

IPv6 アクセスリスト設定モード

特権モードから `access-list ipv6` コマンドで移行します。VLAN インターフェイスに対してパケットの許可・拒否を行うための、IP アクセスリストを登録・変更できます。

deny

機能 IPv6 アクセスリストに拒否ルールを追加します。

フォーマット [`line <line-num>`]

`deny <proto> <src-addr> <dst-addr> [log]`

`deny { tcp | udp } <src-addr> [<src-por>] <dst-addr> [<dst-port>] [log]`

`deny icmpv6 <src-addr> <dst-addr> [type <icmpv6-type>] [log]`

`no line <line-num>`

パラメーター `line <line-num>`

ルールの行番号を指定します。アクセスリストは若い番号のルールから評価されます。

`<proto>`

プロトコル番号またはプロトコル名を指定します。

`tcp` または `udp` の場合は `<src-por>`、`<src-por>` を指定することができます。

`icmp` の場合は `<icmp-type>` を指定することができます。

`<src-addr>`

送信元 IP アドレスを指定します。`any` を指定した場合は全ての IP アドレスにマッチします。

`<src-por>`

送信元ポート番号を指定します。

`<dst-addr>`

宛先 IP アドレスを指定します。`any` を指定した場合は全ての IP アドレスにマッチします。

`<dst-port>`

宛先ポート番号を指定します。

`type <icmpv6-type>`

ICMP タイプを指定します。

`log`

ルールにマッチしたときにログを出力します。

permit

機能 IPv6 アクセスリストに許可ルールを追加します。

フォーマット [`line` *<line-num>*]

`permit` *<proto>* *<src-addr>* *<dst-addr>*

`permit` { `tcp` | `udp` } *<src-addr>* [*<src-por>*] *<dst-addr>* [*<dst-port>*]

`permit icmpv6` *<src-addr>* *<dst-addr>* [`type` *<icmpv6-type>*]

`no line` *<line-num>*

パラメーター 設定パラメーターについては `deny` コマンドを参照してください。

解説 `permit` コマンドでは `log` オプションを指定することはできません。

MAC アクセスリスト設定モード

特権モードから `access-list mac` コマンドで移行します。イーサネットポートに対してパケットの許可・拒否を行うための、MAC アクセスリストを登録・変更できます。

deny

機能 MAC アクセスリストに拒否ルールを追加します。

フォーマット [`line <line-num>`]
`deny <src-addr> <dst-addr> [type <ether-type>] [log]`

`no line <line-num>`

パラメーター `line <line-num>`

ルールの行番号を指定します。アクセスリストは若い番号のルールから評価されます。

`<src-addr>`

送信元 MAC アドレスを指定します。**any** を指定した場合は全ての MAC アドレスにマッチします。

`<dst-addr>`

宛先 MAC アドレスを指定します。**any** を指定した場合は全ての MAC アドレスにマッチします。

`type <ether-type>`

イーサネットタイプを指定します。

`log`

ルールにマッチしたときにログを出力します。

permit

機能 MAC アクセスリストに許可ルールを追加します。

フォーマット [**line** <line-num>]
permit <src-addr> <dst-addr> [**type** <ether-type>]
no line <line-num>

パラメーター 設定パラメーターについては **deny** コマンドを参照してください。

解説 **permit** コマンドでは **log** オプションを指定することはできません。

IPFW VLAN リスト設定モード

特権モードから `ipfw vlan` コマンドで移行します。VLAN インターフェースに対して送信/受信パケットの許可・拒否を行うための、IPFW VLAN リストを登録・変更できます。

deny

機能 IPFW VLAN リストに拒否ルールを追加します。

フォーマット `[line <line-num>] deny { in | out } { icmp | icmp6 } <src-addr> <dst-addr> [type <ether-type>] [log]`

`[line <line-num>] deny { in | out } { ip | ip6 } [proto <proto>] <src-addr> <dst-addr> [log]`

`[line <line-num>] deny { in | out } { tcp | tcp6 | udp | udp6 } <src-addr> [{ eq <src-port> } | { ne <src-port> } | { range <src-port-start> <src-port-end> }] <dst-addr> [{ eq <dst-port> } | { ne <dst-port> } | { range <dst-port-start> <dst-port-end> }] [log]`

`no line <line-num>`

パラメーター `line <line-num>`

ルールの行番号を指定します。IPFW リストは若い番号のルールから評価されます。

in

受信パケットに対してルールが適用されます。

out

送信パケットに対してルールが適用されます。

proto <proto>

プロトコル番号またはプロトコル名を指定します。

<src-addr>

送信元 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq <src-port>

指定した送信元ポート番号を拒否します。

ne *<src-port>*

指定した送信元ポート番号以外を拒否します。

range *<src-port-start> <src-port-end>*

指定した範囲の送信元ポート番号を拒否します。

<dst-addr>

宛先 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq *<dst-port>*

指定した宛先ポート番号を拒否します。

ne *<dst-port>*

指定した宛先ポート番号以外を拒否します。

range *<dst-port-start> <dst-port-end>*

指定した範囲の宛先ポート番号を拒否します。

type *<icmp-type>*

ICMP タイプを指定します。

log

ルールにマッチしたときにログを出力します。

no line *<line-num>*

指定された行番号のルールを削除します。

permit

機能 IPFW VLAN リストに許可ルールを追加します。

フォーマット `[line <line-num>] permit { in | out } { icmp | icmp6 } <src-addr> <dst-addr> [type <icmp-type>] [keep-state]`

`[line <line-num>] permit { in | out } { ip | ip6 } [proto <proto>] <src-addr> <dst-addr>`

`[line <line-num>] permit { in | out } { tcp | tcp6 } <src-addr> [{ eq <src-port> } | { ne <src-port> } | { range <src-port-start> <src-port-end> }] <dst-addr> [{ eq <dst-port> } | { ne <dst-port> } | { range <dst-port-start> <dst-port-end> }] [{ setup [keep-state] } | established]`

`[line <line-num>] permit { in | out } { udp | udp6 } <src-addr> [{ eq <src-port> } | { ne <src-port> } | { range <src-port-start> <src-port-end> }] <dst-addr> [{ eq <dst-port> } | { ne <dst-port> } | { range <dst-port-start> <dst-port-end> }] [keep-state]`

`no line <line-num>`

パラメーター `line <line-num>`

ルールの行番号を指定します。IPFW リストは若い番号のルールから評価されます。

in

受信パケットに対してルールが適用されます。

out

送信パケットに対してルールが適用されます。

proto <proto>

プロトコル番号またはプロトコル名を指定します。

<src-addr>

送信元 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq <src-port>

指定した送信元ポート番号を拒否します。

ne <src-port>

指定した送信元ポート番号以外を拒否します。

range *<src-port-start> <src-port-end>*

指定した範囲の送信元ポート番号を拒否します。

<dst-addr>

宛先 IP アドレスを指定します。 **any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq *<dst-port>*

指定した宛先ポート番号を拒否します。

ne *<dst-port>*

指定した宛先ポート番号以外を拒否します。

range *<dst-port-start> <dst-port-end>*

指定した範囲の宛先ポート番号を拒否します。

type *<icmp-type>*

ICMP タイプを指定します。

setup

コネクション確立要求(SYN=1)の TCP パケットにマッチします。

keep-state

マッチした場合に動的ルールを作成します。

established

RST または ACK ビットがセットされている TCP パケットにマッチします。

no line *<line-num>*

指定された行番号のルールを削除します。

解 説 **permit** コマンドでは **log** オプションを指定することはできません。

IPFW イーサネットポートリスト設定モード

特権モードから ipfw ethport コマンドで移行します。イーサネットポートに対して受信パケットの許可・拒否を行うための、IPFW イーサネットポートリストを登録・変更できます。

deny

機能 IPFW イーサネットポートリストに拒否ルールを追加します。

フォーマット [line <line-num>] deny in { icmp | icmp6 } <src-addr> <dst-addr> [type <ether-type>] [log]

[line <line-num>] deny in { ip | ip6 } [proto <proto>] <src-addr> <dst-addr> [log]

[line <line-num>] deny in { tcp | tcp6 | udp | udp6 } <src-addr> [{ eq <src-port> } | { ne <src-port> } | { range <src-port-start> <src-port-end> }] <dst-addr> [{ eq <dst-port> } | { ne <dst-port> } | { range <dst-port-start> <dst-port-end> }] [log]

no line <line-num>

パラメーター line <line-num>

ルールの行番号を指定します。IPFW リストは若い番号のルールから評価されます。

in

受信パケットに対してルールが適用されます。

proto <proto>

プロトコル番号またはプロトコル名を指定します。

<src-addr>

送信元 IP アドレスを指定します。any を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq <src-port>

指定した送信元ポート番号を拒否します。

ne <src-port>

指定した送信元ポート番号以外を拒否します。

range *<src-port-start> <src-port-end>*

指定した範囲の送信元ポート番号を拒否します。

<dst-addr>

宛先 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq *<dst-port>*

指定した宛先ポート番号を拒否します。

ne *<dst-port>*

指定した宛先ポート番号以外を拒否します。

range *<dst-port-start> <dst-port-end>*

指定した範囲の宛先ポート番号を拒否します。

type *<icmp-type>*

ICMP タイプを指定します。

log

ルールにマッチしたときにログを出力します。

no line *<line-num>*

指定された行番号のルールを削除します。

permit

機能 IPFW イーサネットポートリストに許可ルールを追加します。

フォーマット [**line** <line-num>] **permit in** { **icmp** | **icmp6** } <src-addr> <dst-addr> [**type** <icmp-type>] [**keep-state**]

ット [**line** <line-num>] **permit in** { **ip** | **ip6** } [**proto** <proto>] <src-addr> <dst-addr>

[**line** <line-num>] **permit in** { **tcp** | **tcp6** } <src-addr> [{ **eq** <src-port> } | { **ne** <src-port> } | { **range** <src-port-start> <src-port-end> }] <dst-addr> [{ **eq** <dst-port> } | { **ne** <dst-port> } | { **range** <dst-port-start> <dst-port-end> }] [{ **setup** [**keep-state**] } | **established**]

[**line** <line-num>] **permit in** { **udp** | **udp6** } <src-addr> [{ **eq** <src-port> } | { **ne** <src-port> } | { **range** <src-port-start> <src-port-end> }] <dst-addr> [{ **eq** <dst-port> } | { **ne** <dst-port> } | { **range** <dst-port-start> <dst-port-end> }] [**keep-state**]

no line <line-num>

パラメーター **line** <line-num>

ルールの行番号を指定します。IPFW リストは若い番号のルールから評価されます。

in

受信パケットに対してルールが適用されます。

proto <proto>

プロトコル番号またはプロトコル名を指定します。

<src-addr>

送信元 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq <src-port>

指定した送信元ポート番号を拒否します。

ne <src-port>

指定した送信元ポート番号以外を拒否します。

range <src-port-start> <src-port-end>

指定した範囲の送信元ポート番号を拒否します。

<dst-addr>

宛先 IP アドレスを指定します。**any** を指定した場合は全ての IP アドレスにマッチします。

me を指定した場合は自局 IP アドレスにマッチします。

eq <dst-port>

指定した宛先ポート番号を拒否します。

ne <dst-port>

指定した宛先ポート番号以外を拒否します。

range <dst-port-start> <dst-port-end>

指定した範囲の宛先ポート番号を拒否します。

type <icmp-type>

ICMP タイプを指定します。

setup

コネクション確立要求(SYN=1)の TCP パケットにマッチします。

keep-state

マッチした場合に動的ルールを作成します。

established

RST または ACK ビットがセットされている TCP パケットにマッチします。

no line <line-num>

指定された行番号のルールを削除します。

解 説 **permit** コマンドでは **log** オプションを指定することはできません。

SSL 証明書自動更新設定モード

特権モードから cert-update コマンドで移行します。証明書自動更新の設定を登録・変更できます。

check-fqdn

機能 証明書の fqdn を確認します。

フォーマット [no] check-fqdn

パラメーター

解説 ダウンロードした証明書の CN が csr fqdn コマンドで指定したものと一致するか確認します。

CSR 無しモードでも、一致の確認をする場合 csr fqdn を指定する必要があります。

本コマンドを設定した場合、証明書のダウンロード完了前に csr fqdn を変更すると証明書自動更新が進まなくなりますのでご注意ください。

csr

機能 CSR(証明書署名要求)の各項目を設定します。

フォーマット [no] csr { city | country | email | fqdn | keylen | organization | state }

パラメーター

city	市区町村名を指定します。
country	国を 2 文字で指定します。(日本の場合は JP)
email	メールアドレスを指定します。
fqdn	コモンネーム(fqdn または ip アドレス)を指定します。
keylen	鍵長を指定します。 RSA 鍵(1024,2048,4096)、ECC 鍵(256,384)
organization	組織名を指定します。
state	都道府県を指定します。

解説 country 以外は最大 64 文字です。
CSR ありモードのとき、country と fqdn は必須となります。

csr-update

機能 証明書更新のタイミングを設定します。

フォーマット `csr-update <num>`

パラメーター Num 0~90

証明書の期限切れの何日前に更新作業(CSR 作成)を始めるかを指定します。

解説 0以外を指定すると CSR ありモードとなり、証明書の期限切れの何日前に更新作業(CSR 作成)を始めるかを指定します。

0のときは CSR 無しモードとなり、鍵と証明書を同時にダウンロードする動作となります。

enable

機能 自動更新を開始／停止します。

フォーマット [no] enable

パラメーター

解説 必要な設定が揃ったら enable にして下さい。
一時的に進行を止めたいときにも使用できます。

get-account

- 機 能** アカウントを指定します。
- フォーマット** [no] get-account <str>
- パラメーター** str
アカウント名 最大 64 文字
- 解 説** ユーザー認証を使用する場合は、アップロード/ダウンロードするアカウントを指定します。
使用できる認証方式は、Basic 認証または Digest 認証です。

get-password

機 能 アカウントのパスワードを指定します。

フォーマット [no] get-password <str>

パラメーター str
パスワード 最大 64 文字

解 説 ユーザー認証使用時、アップロード／ダウンロードするアカウントのパスワードを指定します。

get-url

- 機能** ダウンロードする url を指定します。
- フォーマット** [no] get-url <url>
- パラメーター** url
証明書(と鍵)と中間証明書があるフォルダの url 最大 512 文字
指定できるプロトコルは http:// または https:// です。
- 解説** サーバー上に設置される各ファイルは、以下のファイル名である必要があります。また、PEM フォーマットである必要があります。
証明書 : cert.pem
中間証明書 : chain.pem
中間証明書 2 段目 : chain2.pem
秘密鍵 : key.pem ※CSR なしモード時のみ

init

機能 自動更新状態を初期化します。

フォーマット init

パラメーター

解説 CSR ありモードのとき、CSR 作成からやり直します。
ただし、正常な証明書のダウンロードが完了した後は初期化できません。

intermediate-cert-num

機能 中間証明書数を指定します。

フォーマット `intermediate-cert-num <num>`

パラメーター `<num>`
ダウンロードする中間証明書数 0~2

解説 1,2 を指定した場合、ダウンロード元から `chain.pem`, (`chain2.pem`) が取得できるまで、証明書自動更新は進みませんのでご注意ください。

key-password

機能 秘密鍵のパスワードを設定します。

フォーマット [no] key-password <str>

パラメーター <str>

秘密鍵のパスワード 最大 64 文字

解説 秘密鍵にパスワードが掛けられているときに設定します。
パスワードがないときは不要です。

put-url

- 機能** CSR をアップロードする url を指定します。
- フォーマット** [no] put-url <url>
- パラメーター** <url>
CSR をアップロードする url 最大 512 文字
指定できるプロトコルは http:// または https:// です。
- 解説** フォルダ名ではなく、put した csr.pem ファイルをサーバーのローカルストレージに保存するためのスクリプトを指定してください。

SEIKO

セイコーソリューションズ株式会社
〒261-8507 千葉県千葉市美浜区中瀬 1-8
support@seiko-sol.co.jp