

Cisco SD-Routing Enterprise Security SSL Proxy Yang Commands

- Enterprise security SSL proxy yang commands, on page 2

Enterprise security SSL proxy yang commands

These SSL proxy commands are qualified to use with Cisco SD-Routing devices on Cisco SD-WAN Manager.

Example configuration for enterprise security SSL proxy

```
  sd-routing
   enable
   system-ip            172.16.255.16
   site-id              400
   organization-name    "vIPtela Inc Regression"
   vbond name vbond
   wan-interface GigabitEthernet1
   !
   config-template-name VM6-CG
  !
  sslproxy
   enable
   ca-cert-bundle       /bootflash/vmanage-admin/sslProxyDefaultCAbundle.pem
   rsa-key-modulus      2048
   certificate-lifetime 1
   eckey-type           P256
   ca-tp-label          PROXY-SIGNING-CA
   settings expired-certificate  decrypt
   settings untrusted-certificate decrypt
   settings certificate-revocation-check none
   settings unsupported-protocol-versions drop
   settings unsupported-cipher-suites drop
   settings failure-mode         close
   settings minimum-tls-ver      TLSv1
  !
  memory free low-watermark processor 225112
  service timestamps debug datetime msec
  service timestamps log datetime msec
  no service tcp-small-servers
  no service udp-small-servers
  platform console serial
  platform qfp utilization monitor load 80
  platform sslvpn use-pd
  hostname vm6
  enable secret 9 $9$smaK7BO8DMjHMk$OjOtm7rOUv5Yk4lOAHMjVGJak7dIJYCQ7TsErbwkHMM
  username admin privilege 15 secret 9
$9$0mZUAUfuU.hLUE$YWjsVetm4y4i/VikZv3cGN5yQcVvdRlp1mUetVYLl4U
  vrf definition Mgmt-intf
   address-family ipv4
    exit-address-family
   !
   address-family ipv6
    exit-address-family
   !
  !
  no ip finger
  no ip rcmd rcp-enable
  no ip rcmd rsh-enable
  no ip dhcp use class
  ip host vbond 10.0.12.26 2001:a0:c::1a
  ip route 0.0.0.0 0.0.0.0 10.1.14.13
  ip scp server enable
  ip ssh pubkey-chain
   username admin
    key-hash ssh-rsa 493AD24794ED9657FE2F2550CEB48CDA tester@sdwan-ra-vtest
```

```
  !
 !
!
ip ssh bulk-mode 131072
ip tcp RST-count 10 RST-window 5000
ip access-list extended SP-VM6_123202412748732_0-seq-Rule1-acl_
 11 permit object-group zbfw_svc any any
!
ip access-list extended health_probes_accesslist
 10 permit udp any eq 3367 any eq 3367
!
ip http authentication local
ip http server
ip http secure-server
ip http client source-interface GigabitEthernet5
no ip http ctc authentication
no ip rsvp signalling rate-limit
ipv6 unicast-routing
ipv6 route ::/0 2001:a1:e::d
class-map type inspect match-all SP-VM6_123202412748732_0-seq-Rule1-cm_
 match access-group name SP-VM6_123202412748732_0-seq-Rule1-acl_
!
class-map match-all health_probes_cmap
 match access-group name health_probes_accesslist
!
policy-map type inspect SP-VM6_123202412748732_0
 class type inspect SP-VM6_123202412748732_0-seq-Rule1-cm_
   inspect AIP-VM4-pmap_
 !
 class class-default
   drop
 !
!
policy-map health_probes_pmap
 class health_probes_cmap
  priority level 1
 !
!
interface GigabitEthernet1
 no shutdown
 ip address <removed>
 ipv6 address <removed>
 negotiation auto
 zone-member security Local_LAN
exit
interface GigabitEthernet2
 no shutdown
 ip address <removed>
 ipv6 address <removed>
 negotiation auto
 zone-member security Remote-WAN
exit
interface GigabitEthernet3
 no shutdown
 ip address <removed>
 ipv6 address <removed>
 negotiation auto
exit
interface GigabitEthernet4
 no shutdown
 ip address <removed>
 ipv6 address <removed>
 negotiation auto
exit
```

```
interface GigabitEthernet5
 no shutdown
 vrf forwarding Mgmt-intf
 ip address <removed>
 ip dhcp client client-id ascii 9KLLRDXK1VM
 ipv6 address <removed>
 negotiation auto
exit
interface VirtualPortGroup0
 no shutdown
 ip address <removed>
exit
interface VirtualPortGroup1
 no shutdown
 ip address <removed>
 service-policy output health_probes_pmap
exit
interface VirtualPortGroup2
 no shutdown
 ip address <removed>
 service-insertion appqoe
exit
object-group service zbfw_svc
 ip
 exit
!
control-plane
!
no logging console
no logging queue-limit
aaa new-model
aaa authentication enable default enable
aaa authentication login default local
aaa authorization console
aaa authorization exec default local
aaa session-id common
login on-success log
subscriber templating
parameter-map type inspect AIP-VM4-pmap_
 utd-policy AIP-VM4
!
parameter-map type inspect-global
 alert on
 log dropped-packets
 multi-tenancy
 utd-policy AIP-VM4
!
zone security Local_LAN
!
zone security Remote-WAN
!
zone-pair security ZP_Local_LAN_Remote-_-2063742066 source Local_LAN destination Remote-WAN

 service-policy type inspect SP-VM6_123202412748732_0
!
no crypto ikev2 diagnose error
no crypto isakmp diagnose error
crypto pki trustpoint PROXY-SIGNING-CA
 enrollment url bootflash:vmanage-admin/
 fqdn             none
 fingerprint      e88dc0ac7284efd4734d63dd1957eb8355866931
 hash             sha256
 revocation-check none
 rsakeypair PROXY-SIGNING-CA 2048
```

```
 subject-name     CN=C8K-0187c60c-bee4-4015-98a5-73bb67db607f
!
no network-clock revertive
service-insertion appnav-controller-group appqoe ACG-APPQOE
 appnav-controller 192.168.2.1
!
service-insertion service-node-group appqoe SNG-APPQOE
 service-node 192.168.2.2
!
service-insertion service-context appqoe/1
 appnav-controller-group ACG-APPQOE
 service-node-group      SNG-APPQOE
 cluster-type            integrated-service-node
 enable
 vrf global
!
fhrp version vrrp v2
line aux 0
!
line con 0
 exec-timeout 0
 stopbits 1
!
line vty 0 4
 exec-timeout 0
 ! login local
 transport input ssh
!
line vty 5 15
 ! login local
 transport input ssh
!
iox
app-hosting appid utd
 app-resource package-profile cloud-low
 app-vnic gateway0 virtualportgroup 0 guest-interface 0
  guest-ipaddress 192.1.0.2 netmask 255.255.255.0
 !
 app-vnic gateway1 virtualportgroup 1 guest-interface 1
  guest-ipaddress 192.0.2.2 netmask 255.255.255.252
 !
 start
!
canbus baudrate 125000
diagnostic bootup level minimal
ignition off-timer 300
ignition undervoltage threshold 9 000
no ignition sense
no ignition enable
ignition battery-type 12v
ignition sense-voltage threshold 13 000
utd engine standard unified-policy
 threat-inspection profile IP-VM4
  threat detection
  policy balanced
  logging level err
 exit
 tls-decryption profile VM4-TLS-Profile-tls-profile
  categories decrypt
   abortion
   abused-drugs
   adult-and-pornography
   alcohol-and-tobacco
   auctions
```

```
bot-nets
business-and-economy
cdns
cheating
computer-and-internet-info
computer-and-internet-security
confirmed-spam-sources
cult-and-occult
dating
dead-sites
dynamic-content
educational-institutions
entertainment-and-arts
fashion-and-beauty
financial-services
gambling
games
government
gross
hacking
hate-and-racism
health-and-medicine
home
hunting-and-fishing
illegal
image-and-video-search
individual-stock-advice-and-tools
internet-communications
internet-portals
job-search
keyloggers-and-monitoring
kids
legal
local-information
malware-sites
marijuana
military
motor-vehicles
music
news-and-media
nudity
online-greeting-cards
online-personal-storage
open-http-proxies
p2p
parked-sites
pay-to-surf
personal-sites-and-blogs
philosophy-and-political-advocacy
phishing-and-other-frauds
private-ip-addresses
proxy-avoid-and-anonymizers
questionable
real-estate
recreation-and-hobbies
reference-and-research
religion
search-engines
sex-education
shareware-and-freeware
shopping
social-network
society
spam-urls
```

```
      sports
      spyware-and-adware
      streaming-media
      swimsuits-and-intimate-apparel
      training-and-tools
      translation
      travel
      uncategorized
      unconfirmed-spam-sources
      violence
      weapons
      web-advertisements
      web-based-email
      web-hosting
     exit
     log level error
    exit
    policy AIP-VM4
     tls-decryption profile VM4-TLS-Profile-tls-profile
     tls-decryption action decrypt
     threat-inspection profile IP-VM4
    exit
   exit
  !
 !
```