

# Security CLI Reference

CLI commands for configuring and monitoring security.

### Security CLI Templates

The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allows you to configure intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager. Intent-based CLI template refer to the command line interface configuration that are based on the vEdge device syntax. Using CLI templates, Cisco SD-WAN Manager enables pushing vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in Cisco IOS XE syntax.

*Table 1: Security Policy for UTD*

| CLI Template Configuration | Configuration on the Device |
|---|---|
| policy<br>zone internet<br>vpn 0<br>!<br>zone zone1<br>vpn 1<br>!<br>zone zone2<br>vpn 2<br>!<br>zone-pair ZP_zone1_internet_fw_policy<br>source-zone zone1<br>destination-zone internet<br>zone-policy fw_policy<br>!<br>zone-pair ZP_zone1_zone2_fw_policy<br>source-zone zone1<br>destination-zone zone2<br>zone-policy fw_policy<br>!<br>zone-based-policy fw_policy<br>sequence 1<br>match<br>source-data-prefix-list subnet1<br>!<br>action inspect<br>!<br>!<br>default-action pass<br>!<br>zone-to-nozone-internet deny<br>lists<br>data-prefix-list subnet1<br>ip-prefix 10.0.10.0/24<br>!<br>!<br>url-filtering url_filter<br>web-category-action block<br>web-categories games<br>block-threshold moderate-risk<br>block text<br>"<![CDATA[<h3>Access" to the requested<br>page has been denied]]>"<br>target-vpns 1<br>!<br>intrusion-prevention intrusion_policy<br>security-level connectivity<br>inspection-mode protection<br>log-level err<br>target-vpns 1<br>!<br>failure-mode open<br>!<br>!<br>! | |

| CLI Template Configuration | Configuration on the Device |
| --- | --- |
| | ip access-list extended fw_policy-seq-1-acl_<br>11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any<br>!<br>ip access-list extended utd-nat-acl<br>10 permit ip any any<br>!<br>class-map type inspect match-all fw_policy-seq-1-cm_<br>match access-group name fw_policy-seq-1-acl_<br>!<br>policy-map type inspect fw_policy<br>class fw_policy-seq-1-cm_<br>inspect<br>!<br>class class-default<br>pass<br>!<br>!<br>object-group service fw_policy-seq-1-service-og_<br>ip<br>!<br>parameter-map type inspect-global<br>alert on<br>log dropped-packets<br>multi-tenancy<br>vpn zone security<br>!<br>parameter-map type umbrella global<br>token A5EA676087BF66A42DC4F722C2AFD10D00256274<br>dnscrypt<br>vrf 1<br>dns-resolver umbrella<br>match-local-domain-to-bypass<br>!<br>!<br>zone security internet<br>vpn 0<br>!<br>zone security zone1<br>vpn 1<br>!<br>zone security zone2<br>vpn 2<br>!<br>zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet<br>service-policy type inspect fw_policy<br>!<br>zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2<br>service-policy type inspect fw_policy<br>!<br>app-hosting appid utd<br>app-resource package-profile cloud-low<br>app-vnic gateway0 virtualportgroup 0 |

| CLI Template Configuration | Configuration on the Device |
|---|---|
| | guest-interface 0<br>  guest-ipaddress 192.168.1.2 netmask 255.255.255.252<br>  !<br>  app-vnic gateway1 virtualportgroup 1 guest-interface 1<br>  guest-ipaddress 192.0.2.2 netmask 255.255.255.252<br>  !<br>  start<br>  !<br>  utd multi-tenancy<br>  utd engine standard multi-tenancy<br>  web-filter block page profile block-url_filter<br>  text <\![CDATA[<h3>Access to the requested page has been denied</h3><p>Please contact your Network Administrator</p>]]><br>  !<br>  web-filter url profile url_filter<br>  categories block<br>  games<br>  !<br>  block page-profile block-url_filter<br>  log level error<br>  reputation<br>  block-threshold moderate-risk<br>  !<br>  !<br>  threat-inspection profile intrusion_policy<br><br>  threat protection<br>  policy connectivity<br>  logging level err<br>  !<br>  utd global<br>  !<br>  policy utd-policy-vrf-1<br>  all-interfaces<br>  vrf 1<br>  threat-inspection profile intrusion_policy<br><br>  web-filter url profile url_filter<br>  exit<br>  ! |

### Security Monitoring Commands

- **show control connections**