



# Security CLI Reference

---

CLI commands for configuring and monitoring security.

## Security CLI Templates

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

Table 1: Security Policy for UTD

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

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

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

## Security Monitoring Commands

- `show control connections`