# v.1.15.3.



AAA (Authentication, Authorization, Accounting) — .

- Authentication () — () . , .
- Authorization (, , ) — .
- Accounting () — .

| | | | |
|---|---|---|---|
| 1 | local . | **wlc-30(config)# aaa authentication login { default \| <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – , 31 .<br><br>:<br>• local – ;<br>• tacacs – TACACS-;<br>• radius – RADIUS-;<br>• ldap – LDAP-. |
| 2 | enable . | **wlc-30(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ]**<br><br>**[ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – , 31 .<br><br>:<br>• local – ;<br>• tacacs – TACACS-;<br>• radius – RADIUS-;<br>• ldap – LDAP-. |

| | | | |
|---|---|---|---|
| 3 | ( ). | **wlc-30(config)# aaa authentication mode <MODE>** | <MODE> – :<br>• chain – FAIL, ;<br>• break – FAIL, . , .<br>: chain. |
| 4 | ( ). | **wlc-30(config)# aaa authentication attempts max-fail <COUNT> <TIME>** | <COUNT> – , , [1..65535];<br><TIME> – , , [1..65535].<br>:<br><COUNT> – 5; <TIME> – 300 |
| 5 | admin ( ). | **wlc-30(config)# security passwords default-expired** | |
| 6 | ( ). | **wlc-30(config)# security passwords history <COUNT>** | <COUNT> – , . [1..15].<br>: 0 |
| 7 | ( ). | **wlc-30(config)# security passwords lifetime <TIME>** | <TIME> – . [1..365].<br>: . |
| 8 | ENABLE- ( ). | **wlc-30(config)# security passwords min-length <NUM>** | <NUM> – . [8..128].<br>: 0 |
| 9 | ENABLE- ( ). | **wlc-30(config)# security passwords max-length <NUM>** | <NUM> – . [8..128].<br>: . |
| 10 | , ENABLE- ( ). | **wlc-30(config)# security passwords symbol-types <COUNT>** | <COUNT> – . [1..4].<br>: 1 |
| 11 | ENABLE- ( ). | **wlc-30(config)# security passwords lower-case <COUNT>** | <COUNT> – ENABLE-. [0..128].<br>: 0 |
| 12 | () ENABLE- ( ). | **wlc-30(config)# security passwords upper-case <COUNT>** | <COUNT> – () . [0..128].<br>: 0 |
| 13 | ENABLE- ( ). | **wlc-30(config)# security passwords numeric-count <COUNT>** | <COUNT> – . [0..128].<br>: 0 |
| 14 | ENABLE- ( ). | **wlc-30(config)# security passwords special-case <COUNT>** | <COUNT> – . [0..128].<br>: 0 |
| 15 | . | **wlc-30(config)# username <NAME>** | <NAME> – , 31 . |
| 16 | . | **wlc-30(config-user)# password { <CLEAR-TEXT> \| encrypted <HASH_SHA512> }** | <CLEAR-TEXT> – , [8 .. 32] , [0-9a-fA-F];<br><HASH_SHA512> – sha512, 110 . |
| 17 | . | **wlc-30(config-user)# privilege <PRIV>** | <PRIV> – . [1..15]. |
| 18 | . | **wlc-30(config)# line console**<br>**wlc-30(config)# line telnet**<br>**wlc-30(config)# line ssh** | |
| 19 | . | **wlc-30(config-line-ssh)# login authentication <NAME>** | <NAME> – , 31 . |
| 20 | . | **wlc-30(config-line-ssh)# enable authentication <NAME>** | <NAME> – , 31 . |
| 21 | , . | **wlc-30(config-line-ssh)# exec-timeout <SEC>** | <SEC> – , [1..65535]. |

## AAA RADIUS

| | | | |
|---|---|---|---|
| 1 | DSCP IP- RADIUS- ( ). | **wlc-30(config)# radius-server dscp <DSCP>** | <DSCP> – DSCP, [0..63].<br>: 63. |
| 2 | RADIUS- ( ). | **wlc-30(config)# radius-server retransmit <COUNT>** | <COUNT> – RADIUS-, [1..10].<br>: 1. |

| | | | |
|---|---|---|---|
| 3 | , , RADIUS- ( ). | **wlc-30(config)# radius-server timeout <SEC>** | <SEC> – , [1..30].<br><br>: 3 . |
| 4 | RADIUS- . | **wlc-30(config)# radius-server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ] wlc-30(config-radius-server)#** | <IP-ADDR> – IP- RADIUS-, AAA.BBB.CCC.DDD, [0..255];<br><br><IPV6-ADDR> – IPv6- RADIUS-, X:X:X:X::X, [0.. FFFF]<br><br><VRF> – VRF, 31 . |
| 5 | ( ). | **aaa authentication attempts max-fail <COUNT> <TIME>** | <COUNT> – , , [1..65535];<br><br><TIME> – , , [1..65535].<br><br>:<br><br><COUNT> – 5; <TIME> – 300 |
| 6 | RADIUS-. | **wlc-30(config-radius-server)# key ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }** | <TEXT> – [8..16] ASCII-;<br><br><ENCRYPTED-TEXT> – , [8..16] , [16..32] . |
| 7 | RADIUS- ( ). | **wlc-30(config-radius-server)# priority <PRIORITY>** | <PRIORITY> – , [1..65535].<br><br>, .<br><br>: 1. |
| 8 | , , RADIUS- ( ). | **wlc-30(config-radius-server)# timeout <SEC>** | <SEC> – , [1..30].<br><br>: . |
| 9 | IPv4/IPv6-, IP/IPv6-RADIUS-. | **wlc-30(config-radius-server)# source-address { <ADDR> \| <IPV6-ADDR> }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><br><IPV6-ADDR> – IPv6- , X:X:X:X::X, [0..FFFF]. |
| 10 | radius . | **wlc-30(config)# aaa authentication login { default \| <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – , 31 .<br><br>:<br><br>• local – ;<br>• tacacs – TACACS-;<br>• radius – RADIUS-;<br>• ldap – LDAP-. |
| 11 | radius . | **wlc-30(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – 31 ;<br><br>• default – .<br><br><METHOD> – :<br><br>• enable – enable-;<br>• tacacs – TACACS;<br>• radius – RADIUS;<br>• ldap – LDAP. |
| 12 | ( ). | **wlc-30(config)# aaa authentication mode <MODE>** | <MODE> – :<br><br>• chain – FAIL, ;<br>• break – FAIL, . , .<br><br>: chain. |
| 13 | radius ( ). | **wlc-30(config)# aaa accounting login start-stop <METHOD 1> [ <METHOD 2> ]** | <METHOD> – :<br><br>• tacacs – TACACS;<br>• radius – RADIUS. |
| 14 | . | **wlc-30(config)# line <TYPE>** | <TYPE> – :<br><br>• console – ;<br>• ssh – . |
| 15 | . | **wlc-30(config-line-console)# login authentication <NAME>** | <NAME> – , 31 . 8. |
| 16 | . | **wlc-30(config-line-console)# enable authentication <NAME>** | <NAME> – , 31 . 9. |

## AAA TACACS

| | | | |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | DSCP IP- TACACS- ( ). | **wlc-30(config)# tacacs-server dscp <DSCP>** | <DSCP> – DSCP, [0..63].<br><br>: 63. |
| 2 | , , TACACS- ( ). | **wlc-30(config)# tacacs-server timeout <SEC>** | <SEC> – , [1..30].<br><br>: 3 . |
| 3 | TACACS- . | **wlc-30(config)# tacacs -server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ]**<br><br>**wlc-30(config-tacacs-server)#** | <IP-ADDR> – IP- TACACS-, AAA.BBB.CCC. DDD, [0..255]<br><br><IPV6-ADDR> – IPv6- TACACS-, X:X:X:X::X, [0..FFFF]<br><br><VRF> – VRF, 31 . |
| 4 | ( ). | **aaa authentication attempts max-fail <COUNT> <TIME>** | <COUNT> – , , [1..65535];<br><br><TIME> – , , [1..65535].<br><br>:<br><br><COUNT> – 5; <TIME> – 300 |
| 5 | TACACS-. | **wlc-30(config-tacacs-server)# key ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }** | <TEXT> – [8..16] ASCII-;<br><br><ENCRYPTED-TEXT> – , [8..16] , [16..32] . |
| 6 | c TACACS- ( ). | **wlc-30(config-tacacs-server)# port <PORT>** | <PORT> – TCP- c , [1..65535].<br><br>: 49 TACACS-. |
| 7 | TACACS- ( ). | **wlc-30(config-tacacs-server)# priority <PRIORITY>** | <PRIORITY> – , [1..65535].<br><br>, .<br><br>: 1. |
| 8 | IPv4/IPv6-, IP/IPv6- TACACS-. | **wlc-30(config-tacacs-server)# source-address { <ADDR> \| <IPV6-ADDR> }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255]. |
| 9 | TACACS . | **wlc-30(config)# aaa authentication enable <NAME><METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – 31 ;<br><br>• default – .<br><br><METHOD> – :<br><br>• enable – enable-;<br>• tacacs – TACACS;<br>• radius – RADIUS;<br>• ldap – LDAP. |
| 10 | ( ). | **wlc-30(config)# aaa authentication mode <MODE>** | <MODE> – :<br><br>• chain – FAIL, ;<br>• break – FAIL, . , .<br><br>: chain. |
| 11 | , CLI ( ). | **wlc-30(config)# aaa accounting commands stop-only tacacs** | |
| 12 | tacacs ( ). | **wlc-30(config)# aaa accounting login start-stop <METHOD 1> [ <METHOD 2> ]** | <METHOD> – :<br><br>• tacacs – TACACS;<br>• radius – RADIUS. |
| 13 | . | **wlc-30(config)# line <TYPE>** | <TYPE> – :<br><br>• console – ;<br>• ssh – . |
| 14 | . | **wlc-30(config-line-console)# login authentication <NAME>** | <NAME> – , 31 . 7. |
| 15 | . | **wlc-30(config-line-console)# enable authentication <NAME>** | <NAME> – , 31 . 8. |

## AAA LDAP

| | | | |
|---|---|---|---|
| 1 | DN (Distinguished name), . | **wlc-30(config)# ldap-server base-dn <NAME>** | <NAME> – DN, 255 . |
| 2 | , , LDAP- ( ). | **wlc-30(config)# ldap-server bind timeout <SEC>** | <SEC> – , [1..30].<br><br>: 3 . |

| | | | |
|---|---|---|---|
| 3 | DN (Distinguished name) , LDAP- . | **wlc-30(config)# ldap-server bind authenticate root-dn <NAME>** | <NAME> – DN , 255 . |
| 4 | , LDAP- . | **wlc-30(config)# ldap-server bind authenticate root-password ascii-text { <TEXT> \| encrypted <ENCRYPTED-TEXT> }** | <TEXT> – [8..16] ASCII-;<br><ENCRYPTED-TEXT> – , [8..16] , [16..32] . |
| 5 | , LDAP- ( ). | **wlc-30(config)# ldap-server search filter user-object-class <NAME>** | <NAME> – , 127 .<br>: posixAccount. |
| 6 | LDAP- ( ). | **wlc-30(config)# ldap-server search scope <SCOPE>** | <SCOPE> – LDAP-, :<br>• onelevel – DN LDAP-;<br>• subtree – DN LDAP .<br>: subtree. |
| 7 | , , LDAP- , ( ). | **wlc-30(config)# ldap-server search timeout <SEC>** | <SEC> – , [0..30]<br>: 0 – LDAP-. |
| 8 | , LDAP- ( ). | **wlc-30(config)# ldap-server naming-attribute <NAME>** | <NAME> – , 127 .<br>: uid. |
| 9 | , ( ). | **wlc-30(config)# ldap-server privilege-level-attribute <NAME>** | <NAME> – , 127 .<br>: priv-lvl |
| 10 | DSCP IP- LDAP- ( ). | **wlc-30(config)# ldap-server dscp <DSCP>** | <DSCP> – DSCP, [0..63].<br>: 63 |
| 11 | LDAP- . | **wlc-30(config)# ldap -server host { <IP-ADDR> \| <IPV6-ADDR> } [ vrf <VRF> ]**<br>**wlc-30(config-ldap-server)#** | <IP-ADDR> – IP- LDAP-, AAA.BBB.CCC.DDD, [0..255]<br><IPV6-ADDR> – IPv6- LDAP-, X:X:X:X::X, [0.. FFFF]<br><VRF> – VRF, 31 . |
| 12 | ( ) | **aaa authentication attempts max-fail <COUNT> <TIME>** | <COUNT> – , , [1..65535];<br><TIME> – , , [1..65535].<br>:<br><COUNT> – 5; <TIME> – 300 |
| 13 | c LDAP- ( ). | **wlc-30(config-ldap-server)# port <PORT>** | <PORT> – TCP- c , [1..65535].<br>: 389 LDAP-. |
| 14 | LDAP- ( ). | **wlc-30(config-ldap-server)# priority <PRIORITY>** | <PRIORITY> – , [1..65535].<br>, .<br>: 1. |
| 15 | IPv4/IPv6-, IP/IPv6- LDAP-. | **wlc-30(config-ldap-server)# source-address { <ADDR> \| <IPV6-ADDR> }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><IPV6-ADDR> – IPv6- , X:X:X:X::X, [0..FFFF]. |
| 16 | LDAP . | **wlc-30(config)# aaa authentication login { default \| <NAME> } <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – , 31 .<br>:<br>• local – ;<br>• tacacs – TACACS-;<br>• radius – RADIUS-;<br>• ldap – LDAP-. |
| 17 | LDAP . | **wlc-30(config)# aaa authentication enable <NAME> <METHOD 1> [ <METHOD 2> ] [ <METHOD 3> ] [ <METHOD 4> ]** | <NAME> – 31 ;<br>• default – .<br><METHOD> – :<br>• enable – enable-;<br>• tacacs – TACACS;<br>• radius – RADIUS;<br>• ldap – LDAP. |

| | | | |
|---|---|---|---|
| 18 | . | **wlc-30(config)# aaa authentication mode <MODE>** | <MODE> – :<br>• chain – FAIL, ;<br>• break – FAIL, . , .<br>: chain. |
| 19 | . | **wlc-30(config)# line <TYPE>** | <TYPE> – :<br>• console – ;<br>• ssh – . |
| 20 | . | **wlc-30(config-line-console)# login authentication <NAME>** | <NAME> – , 31 . 14. |
| 21 | . | **wlc-30(config-line-console)# enable authentication <NAME>** | <NAME> – , 31 . 15. |

### telnet RADIUS-

:

, Telnet, RADIUS (192.168.16.1/24).

:

RADIUS- (password):

```
wlc-30# configure
wlc-30(config)# radius-server host 192.168.16.1
wlc-30(config-radius-server)# key ascii-text encrypted 8CB5107EA7005AFF
wlc-30(config-radius-server)# exit
```

:

```
wlc-30(config)# aaa authentication login log radius
```

, Telnet-:

```
wlc-30(config)# line telnet
wlc-30(config-line-telnet)# login authentication log
wlc-30(config-line-telnet)# exit
wlc-30(config)# exit
```

RADIUS- :

```
wlc-30# show aaa radius-servers
```

:

```
wlc-30# show aaa authentication
```

## Web-

WL-30 web-, Hotspot-. ( ) , web-, .

web- WLC-30 , , Hotspot-. , (, ), . . , .

GUI URL: http://<IP- >:8080/epadmin

, (1-15). , .

- *1-9* — (show ...);
- *10-14* — , ;
- *15* — .

CLI :

```
wlc-30(config)# privilege <COMMAND-MODE> level <PRIV><COMMAND>
```

<COMMAND-MODE> – ;

<PRIV> – , [1..15];

<COMMAND> – , 255 .

:

10, «show interfaces bridges». «show interfaces bridges» 3.

:

, 10 3:

```
wlc-30(config)# privilege root level 3 "show interfaces bridge"
wlc-30(config)# privilege root level 10 "show interfaces"
```

| | | | |
|---|---|---|---|
| 1 | ICMP flood-. | **wlc-30(config)# ip firewall screen dos-defense icmp-threshold { <NUM> }** | <NUM> – ICMP- [1..10000]. |
| 2 | land-. | **wlc-30(config)# firewall screen dos-defense land** | |
| 3 | , | **wlc-30(config)# ip firewall screen dos-defense limit-session-destination { <NUM> }** | <NUM> –<br>IP- [1..10000]. |
| 4 | , | **wlc-30(config)# ip firewall screen dos-defense limit-session-source { <NUM> }** | <NUM> –<br>IP- [1..10000]. |
| 5 | SYN flood-. | **wlc-30(config)# ip firewall screen dos-defense syn-flood { <NUM> } [src-dsr]** | <NUM> – TCP- SYN [1..10000].<br>src-dst – TCP- SYN . |
| 6 | UDP flood-. | **wlc-30(config)# ip firewall screen dos-defense udp-threshold { <NUM> }** | <NUM> – UDP- [1..10000]. |
| 7 | winnuke-. | **wlc-30(config)# ip firewall screen dos-defense winnuke** | |
| 8 | TCP- FIN ACK. | **wlc-30(config)# ip firewall screen spy-blocking fin-no-ack** | |
| 9 | ICMP- . | **wlc-30(config)# ip firewall screen spy-blocking icmp-type** | <TYPE> – ICMP, :<br>• destination-unreachable<br>• echo-request<br>• reserved<br>• source-quench<br>• time-exceeded |
| 10 | IP sweep-. | **wlc-30(config)# ip firewall screen spy-blocking ip-sweep { <NUM> }** | <NUM> – ip sweep-, [1..1000000]. |
| 11 | port scan-. | **wlc-30(config)# ip firewall screen spy-blocking port-scan { <threshold> } [ <TIME> ]** | <threshold> – , port scan- [1..10000].<br><TIME> – [1..1000000]. |
| 12 | IP spoofing-. | **wlc-30(config)# ip firewall screen spy-blocking spoofing** | |

| | | | |
|---|---|---|---|
| 13 | TCP-, SYN FIN. | **wlc-30(config)# ip firewall screen spy-blocking syn-fin** | |
| 14 | TCP-, : FIN, PSH, URG. XMAS. | **wlc-30(config)# ip firewall screen spy-blocking tcp-all-flag** | |
| 15 | TCP-, flags. | **wlc-30(config)# ip firewall screen spy-blocking tcp-no-flag** | |
| 16 | ICMP-. | **wlc-30(config)# ip firewall screen suspicious-packets icmp-fragment** | |
| 17 | IP-. | **wlc-30(config)# ip firewall screen suspicious-packets ip-fragment** | |
| 18 | ICMP- 1024 . | **wlc-30(config)# ip firewall screen suspicious-packets icmp-fragment** | |
| 19 | TCP-, SYN. | **wlc-30(config)# ip firewall screen suspicious-packets syn-fragment** | |
| 20 | UDP-. | **wlc-30(config)# ip firewall screen suspicious-packets udp-fragment** | |
| 21 | , ID IP 137 . | **wlc-30(config)# ip firewall screen suspicious-packets unknown-protocols** | |
| 22 | ( SNMP, syslog CLI) . | **wlc-30(config)# ip firewall logging interval <NUM>** | <NUM> – [30 .. 2147483647] |
| 23 | CLI. | **wlc-30(config)# logging firewall screen detailed** | |
| 24 | DoS- CLI, syslog SNMP. | **wlc-30(config)# logging firewall screen dos-defense <ATACK_TYPE>** | <ATACK_TYPE> – DoS-, : icmp-threshold, land, limit-session-destination, limit-session-source, syn-flood, udp-threshold, winnuke. |
| 25 | CLI, syslog SNMP | **wlc-30(config)# logging firewall screen spy-blocking { <ATACK_TYPE> \| icmp-type <ICMP_TYPE> }** | <ATACK_TYPE> – , : fin-no-ack, ip-sweep, port-scan, spoofing, syn-fin, tcp-all-flag, tcp-no-flag.<br><br><ICMP_TYPE> – ICMP, : destination-unreachable, echo-request, reserved, source-quench, time-exceeded. |
| 26 | CLI, syslog SNMP | **wlc-30(config)# logging firewall screen suspicious-packets <PACKET_TYPE>** | <PACKET_TYPE> – , : icmp-fragment, ip-fragment, large-icmp, syn-fragment, udp-fragment, unknown-protocols. |

| | |
|---|---|
| ip firewall screen dos-defense icmp-threshold | ICMP flood-. ICMP- . - . |
| firewall screen dos-defense land | land-. source destination IP-, SYN TCP. - TCP SYN TCP . |
| ip firewall screen dos-defense limit-session-destination | IP- , ( DoS-: SYN flood, UDP flood, ICMP flood, ..). , , DoS-. |
| ip firewall screen dos-defense limit-session-source | IP- , ( DoS-: SYN flood, UDP flood, ICMP flood, ..). , , DoS-. |
| ip firewall screen dos-defense syn-flood | SYN flood-. TCP- SYN . - TCP SYN TCP-. |
| ip firewall screen dos-defense udp-threshold | UDP flood-. UDP- . - UDP-. |
| ip firewall screen dos-defense winnuke | winnuke-.<br>TCP- URG 139 . Windows ( 95 ). |
| ip firewall screen spy-blocking fin-no-ack | TCP- FIN ACK. . |
| ip firewall screen spy-blocking icmp-type destination-unreachable | ICMP- 3 (destination-unreachable), , . . |
| ip firewall screen spy-blocking icmp-type echo-request | ICMP- 8 (echo-request), , . . |
| ip firewall screen spy-blocking icmp-type reserved | ICMP- 2 7 (reserved), , . . |
| ip firewall screen spy-blocking icmp-type source-quench | ICMP- 4 (source quench), , . . |
| ip firewall screen spy-blocking icmp-type time-exceeded | ICMP- 11 (time exceeded), , . . |
| ip firewall screen spy-blocking ip-sweep | IP sweep-. , 10 ICMP- , 10 , 11 . . |

| | |
|---|---|
| ip firewall screen spy-blocking port-scan | port scan-. (<threshold>) 10 TCP- SYN TCP-, 10 UDP-, UDP-, port scan (<TIME>). . |
| ip firewall screen spy-blocking spoofing | ip spoofing-. . , 10.0.0.1/24 Gi1/0/1, Gi1/0/2, , . source IP-. |
| ip firewall screen spy-blocking syn-fin | TCP- SYN FIN. . |
| ip firewall screen spy-blocking tcp-all-flag | TCP- : FIN, PSH, URG. XMAS. |
| ip firewall screen spy-blocking tcp-no-flag | TCP- flags. . |
| ip firewall screen suspicious-packets icmp-fragment | ICMP-. ICMP- . |
| ip firewall screen suspicious-packets ip-fragment | . |
| ip firewall screen suspicious-packets large-icmp | ICMP- 1024 . |
| ip firewall screen suspicious-packets syn-fragment | TCP- SYN. TCP SYN . . |
| ip firewall screen suspicious-packets udp-fragment | UDP-. |
| ip firewall screen suspicious-packets unknown-protocols | , ID IP 137 . |

:

LAN- WLC-30 land, syn-flood, ICMP flood SNMP SNMP- 192.168.0.10.


:

firewall ( firewall ):

```
wlc-30(config)# security zone LAN
wlc-30(config-zone)# exit
wlc-30(config)# security zone WAN
wlc-30(config-zone)# exit
wlc-30(config)# security zone-pair LAN WAN
wlc-30(config-zone-pair)# rule 100
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# ex
wlc-30(config-zone-pair)# exit
wlc-30(config)# security zone-pair WAN LAN
wlc-30(config-zone-pair)# rule 100
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# interface gigabitethernet 1/0/1
wlc-30(config-if-gi)# security-zone LAN
wlc-30(config-if-gi)# ip address 192.168.0.1/24
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gigabitethernet 1/0/2
wlc-30(config-if-gi)# security-zone WAN
wlc-30(config-if-gi)# ip address 10.0.0.1/24
wlc-30(config-if-gi)# exit
```

land, syn-flood, ICMP flood-:

```
wlc-30(config)# ip firewall screen dos-defense land
wlc-30(config)# ip firewall screen dos-defense syn-flood 100 src-dst
wlc-30(config)# ip firewall screen dos-defense icmp-threshold 100
```

:

```
wlc-30(config)# ip firewall logging screen dos-defense land
wlc-30(config)# ip firewall logging screen dos-defense syn-flood
wlc-30(config)# ip firewall logging screen dos-defense icmp-threshold
```

SNMP-, :

```
wlc-30(config)# snmp-server
wlc-30(config)# snmp-server host 192.168.0.10
```

:

```
wlc-30# show ip firewall screen counters
```

## Firewall

Firewall — , .

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config)# security zone <zone-name1>**<br>**wlc-30(config)# security zone <zone-name2>** | <zone-name> – 12 . |
| 2 | . | **wlc-30(config-zone)# description <description>** | <description> – 255 . |
| 3 | VRF, ( ). | **wlc-30(config- zone)# ip vrf forwarding <VRF>** | <VRF> – VRF, 31 . |
| 4 | NAT Firewall ( , ). | **wlc-30(config)# ip firewall sessions counters** | |
| 5 | , - ( , ). | **wlc-30(config)# ip firewall sessions allow-unknown** | |
| 6 | ( ).<br>stateless. | **wlc-30(config)# ip firewall mode <MODE>** | <MODE> – , : stateful, stateless.<br>: stateful |
| 7 | ( ). | **wlc-30(config)# ip firewall sessions generic-timeout <TIME>** | <TIME> – , [1..8553600].<br>: 60 . |
| 8 | ICMP-, ( ). | **wlc-30(config)# ip firewall sessions icmp-timeout <TIME>** | <TIME> – ICMP-, [1..8553600].<br>: 30 . |
| 9 | ICMPv6-, ( ). | **wlc-30(config)# ip firewall sessions icmpv6-timeout <TIME>** | <TIME> – ICMP-, [1..8553600].<br>: 30 . |
| 10 | ( ). | **wlc-30(config)# ip firewall sessions max-expect <COUNT>** | <COUNT> – , [1..8553600].<br>: 256. |
| 11 | ( ). | **wlc-30(config)# ip firewall sessions max-tracking <COUNT>** | <COUNT> – , [1..8553600].<br>: 512000. |
| 12 | TCP- « », ( ). | **wlc-30(config)# ip firewall sessions tcp-connect-timeout <TIME>** | <TIME> – TCP- " ", [1..8553600].<br>: 60 . |
| 13 | TCP- " ", ( ). | **wlc-30(config)# ip firewall sessions tcp-disconnect-timeout <TIME>** | <TIME> – TCP- " ", [1..8553600].<br>: 30 . |

| | | | |
|---|---|---|---|
| 14 | TCP- " ", ( ). | **wlc-30(config)# ip firewall sessions tcp-established-timeout <TIME>** | <TIME> – TCP- " ", [1..8553600].<br>: 120 . |
| 15 | , TCP- ( ). | **wlc-30(config)# ip firewall sessions tcp-latecome-timeout <TIME>** | <TIME> – , [1..8553600].<br>: 120 . |
| 16 | ( ). | **wlc-30(config)# ip firewall sessions tracking** | <PROTOCOL> – [ftp, h323, pptp, netbios-ns, tftp], .<br><OBJECT-GROUP-SERVICE> – TCP/UDP- sip , 31 . , sip 5060.<br>"all", .<br>– . |
| 17 | UDP- " ", ( ). | **wlc-30(config)# ip firewall sessions udp-assured-timeout <TIME>** | <TIME> – UDP- " ", [1..8553600].<br>: 180 . |
| 18 | UDP- « », . | **wlc-30(config)# ip firewall sessions udp-wait-timeout <TIME>** | <TIME> – UDP- « », [1..8553600].<br>: 30 . |
| 19 | IP-, . | **wlc-30(config)# object-group network <obj-group-name>** | <obj-group-name> – 31 . |
| 20 | IP- ( ). | **wlc-30(config-object-group-network)# description <description>** | <description> – , 255 . |
| 21 | IPv4/IPv6- . | **wlc-30(config-object-group-network)# ip prefix <ADDR/LEN>** | <ADDR/LEN> – , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32]. |
| | | **wlc-30(config-object-group-network)# ip address-range <FROM-ADDR>-<TO-ADDR>** | <FROM-ADDR> – IP- ;<br><TO-ADDR> – IP- , . , IP-.<br>AAA.BBB.CCC.DDD, [0..255]. |
| | | **wlc-30(config-object-group-network)# ipv6 prefix <IPV6-ADDR/LEN>** | <IPV6-ADDR/LEN> – IP- , X:X:X:X::X/EE, X [0..FFFF] EE [1..128]. |
| | | **wlc-30(config-object-group-network)# ipv6 address-range <FROM-ADDR>-<TO-ADDR>** | <FROM-ADDR> – IPv6- ;<br><TO-ADDR> – IPv6- , . , IPv6-.<br>X:X:X:X::X, [0..FFFF]. |
| 22 | , . | **wlc-30(config)# object-group service <obj-group-name>** | <obj-group-name> – , 31 . |
| 23 | ( ). | **wlc-30(config-object-group-service)# description <description>** | <description> – , 255 . |
| 24 | (tcp/udp-) . | **wlc-30(config-object-group-service)# port-range <port>** | <port> – [1..65535].<br>«,» «-». |
| 25 | , DPI. | **wlc-30(config)# object-group application <NAME>** | <NAME> – , 31 . |
| 26 | ( ). | **wlc-30(config-object-group-application)# description <description>** | <description> – , 255 . |
| 27 | . | **wlc-30(config-object-group-application)# application < APPLICATION >** | < APPLICATION > – |
| 28 | (, , E1/Multilink ), (l2tp, openvpn, pptp) (gre, ip4ip4, l2tp, lt, pppoe, pptp) ( ). | **wlc-30(config-if-gi)# security-zone <zone-name>** | <zone-name> – 12 . |
| | Firewall (, , E1/Multilink ), (l2tp, openvpn, pptp) (gre, ip4ip4, l2tp, lt, pppoe, pptp) ( ) | **wlc-30(config-if-gi)# ip firewall disable** | |
| 29 | . | **wlc-30(config)# security zone-pair <src-zone-name1> <dst-zone-name2>** | <src-zone-name> – 12 .<br><dst-zone-name> – 12 . |
| 30 | . | **wlc-30(config-zone-pair)# rule <rule-number>** | <rule-number> – 1..10000. |
| 31 | ( ). | **wlc-30(config-zone-rule)# description <description>** | <description> – 255 . |
| 32 | . | **wlc-30(config-zone-rule)# action <action> [ log ]** | <action> – permit/deny/reject/netflow-sample/sflow-sample<br>log – , . |

| | | | |
|---|---|---|---|
| 33 | IP-, ( ). | **wlc-30(config-zone-rule)# match [not] protocol <protocol-type>** | <protocol-type> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre.<br>«any» . |
| | | **wlc-30(config-zone-rule)# match [not] protocol-id <protocol-id>** | <protocol-id> – IP-, [0x00-0xFF]. |
| 34 | IP- , ( ). | **wlc-30(config-zone-rule)# match [not] source-address <OBJ-GROUP-NETWORK-NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 31 . «any» IP- /. |
| 35 | IP- , ( ). | **wlc-30(config-zone-rule)# match [not] destination-address <OBJ-GROUP-NETWORK-NAME>** | |
| 36 | MAC- , ( ). | **wlc-30(config-zone-rule)# match [not] source-mac <mac-addr>** | <mac-addr> – XX:XX:XX:XX:XX:XX, [00..FF]. |
| 37 | MAC- , ( ). | **wlc-30(config-zone-rule)# match [not] destination-mac <mac-addr>** | |
| 38 | TCP/UDP- , ( ). | **wlc-30(config-zone-rule)# match [not] source-port <PORT-SET-NAME>** | <PORT-SET-NAME> – 31 . «any» TCP /UDP- /. |
| 39 | TCP/UDP- , ( ). | **wlc-30(config-zone-rule)# match [not] destination-port <PORT-SET-NAME>** | |
| 40 | ICMP, ( ICMP) ( ). | **wlc-30(config-zone-rule)# match [not] icmp <ICMP_TYPE> <ICMP_CODE>** | <ICMP_TYPE> – ICMP, [0..255];<br><ICMP_CODE> – ICMP, [0..255]. «any» ICMP. |
| 41 | , , IP- . | **wlc-30(config-zone-rule)# match [not] destination-nat** | |
| 42 | ( , zone-pair any self zone-pair <zone-name> any). | **wlc-30(config-zone-pair-rule)# rate-limit pps <rate-pps>** | <rate-pps> – , . [1..10000]. |
| 43 | IP- ( , zone-pair any self zone-pair <zone-name> any). | **wlc-30(config-zone-pair-rule)# match [not] fragment** | |
| 44 | IP-, ip-option ( , zone-pair any self zone-pair <zone-name> any). | **wlc-30(config-zone-pair-rule)# match [not] ip-option** | |
| 45 | . | **wlc-30(config-zone-rule)# enable** | |

not , .

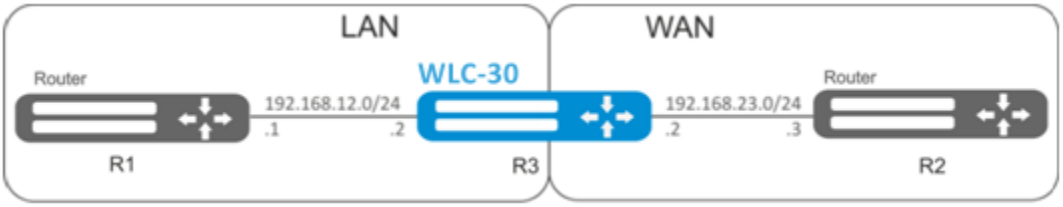
«match» «not». , .

« CLI».

## Firewall

:

ICMP R1, R2 WLC-30.




:

:

```
wlc-30# configure
wlc-30(config)# security zone LAN
wlc-30(config-zone)# exit
wlc-30(config)# security zone WAN
wlc-30(config-zone)# exit
```

:

```
wlc-30(config)# interface gi1/0/2
wlc-30(config-if-gi)# ip address 192.168.12.2/24
wlc-30(config-if-gi)# security-zone LAN
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gi1/0/3
wlc-30(config-if-gi)# ip address 192.168.23.2/24
wlc-30(config-if-gi)# security-zone WAN
wlc-30(config-if-gi)# exit
```

«LAN», , «WAN», «WAN».

```
wlc-30(config)# object-group network WAN
wlc-30(config-object-group-network)# ip address-range 192.168.23.2
wlc-30(config-object-group-network)# exit
wlc-30(config)# object-group network LAN
wlc-30(config-object-group-network)# ip address-range 192.168.12.2
wlc-30(config-object-group-network)# exit
wlc-30(config)# object-group network LAN_GATEWAY
wlc-30(config-object-group-network)# ip address-range 192.168.12.1
wlc-30(config-object-group-network)# exit
wlc-30(config)# object-group network WAN_GATEWAY
wlc-30(config-object-group-network)# ip address-range 192.168.23.3
wlc-30(config-object-group-network)# exit
```

«LAN» «WAN» , ICMP- R1 R2. *enable:*

```
wlc-30(config)# security zone-pair LAN WAN
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# match destination-address WAN_GATEWAY
wlc-30(config-zone-pair-rule)# match source-address LAN_GATEWAY
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair-pair)# exit
```

«WAN» «LAN» , ICMP- R2 R1. *enable:*

```
wlc-30(config)# security zone-pair WAN LAN
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# match destination-address LAN_GATEWAY
wlc-30(config-zone-pair-rule)# match source-address WAN_GATEWAY
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
```

«self». , , «self». , «WAN» «self». , ICMP- R2 , ICMP- «WAN»:

```
wlc-30(config)# security zone-pair WAN self
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# match destination-address WAN
wlc-30(config-zone-pair-rule)# match source-address WAN_GATEWAY
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
```

, «LAN» «self». , ICMP- R1 , ICMP- «LAN»:

```
wlc-30(config)# security zone-pair LAN self
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# match protocol icmp
wlc-30(config-zone-pair-rule)# match destination-address LAN
wlc-30(config-zone-pair-rule)# match source-address LAN_GATEWAY
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# exit
wlc-30(config)# exit
```

:

```
wlc-30# show security zone
```

:

```
wlc-30# show security zone-pair
wlc-30# show security zone-pair configuration
```

:

```
wlc-30# show ip firewall sessions
```

### (DPI)

⚠ - . .

:

youtube, bittorrent facebook.


:

WLC-30 :

```
wlc-30# configure
wlc-30(config)# security zone LAN
wlc-30(config-zone)# exit
wlc-30(config)# security zone WAN
wlc-30(config-zone)# exit
```

:

```
wlc-30(config)# interface gi1/0/1
wlc-30(config-if-gi)# ip address 10.0.0.1/24
wlc-30(config-if-gi)# security-zone WAN
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gi1/0/2
wlc-30(config-if-te)# ip address 192.168.0.1/24
wlc-30(config-if-te)# security-zone LAN
wlc-30(config-if-te)# exit
```

stateless:

```
wlc-30(config)# ip firewall mode stateless
```

, .

```
wlc-30(config)# object-group application APP
wlc-30(config-object-group-application)# application youtube
wlc-30(config-object-group-application)# application bittorrent
wlc-30(config-object-group-application)# application facebook
wlc-30(config-object-group-application)# exit
```

«WAN» «LAN» , , , . *enable:*

```
wlc-30(config)# security zone-pair WAN LAN
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action deny
wlc-30(config-zone-pair-rule)# match application APP
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 2
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair-pair)# exit
```

«LAN» «WAN» , , , . *enable:*

```
wlc-30(config)# security zone-pair LAN WAN
wlc-30(config-zone-pair)# rule 1
wlc-30(config-zone-pair-rule)# action deny
wlc-30(config-zone-pair-rule)# match application APP
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair)# rule 2
wlc-30(config-zone-pair-rule)# action permit
wlc-30(config-zone-pair-rule)# enable
wlc-30(config-zone-pair-rule)# exit
wlc-30(config-zone-pair-pair)# exit
```

:

```
wlc-30# show security zone
```

:

```
wlc-30# show security zone-pair
wlc-30# show security zone-pair configuration
```

:

```
wlc-30# show ip firewall sessions
```

## (ACL)

Access Control List ACL — , , .

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config)# ip access-list extended <NAME>** | <NAME> – , 31 . |
| 2 | ( ). | **wlc-30(config-acl)# description <DESCRIPTION>** | <DESCRIPTION> – , 255 . |
| 3 | . . | **wlc-30(config-acl)# rule <ORDER>** | <ORDER> – , [1..4094]. |
| 4 | , , . | **wlc-30(config-acl-rule)# action <ACT>** | <ACT> – :<br>• permit – ;<br>• deny – . |
| 5 | / , ( ). | **wlc-30(config-acl-rule)# match protocol <TYPE>** | <TYPE> – , : esp, icmp, ah, eigrp, ospf, igmp, ipip, tcp, pim, udp, vrrp, rdp, l2tp, gre. «any» ; |
| | | **wlc-30(config-acl-rule)# match protocol-id <ID>** | <ID> – IP-, [0x00-0xFF]. |
| 6 | IP- , ( ). | **wlc-30(config-acl-rule)# match source-address { <ADDR> <MASK> \| any }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><MASK> – IP-, AAA.BBB.CCC.DDD, [0..255]. , 0, IP-, . «any» IP- /. |
| 7 | IP- , ( ). | **wlc-30(config-acl-rule)# match destination-address { <ADDR> <MASK> \| any }** | |
| 8 | MAC- , ( ). | **wlc-30(config-acl-rule)# match source-mac <ADDR><WILDCARD>** | <ADDR> – - , XX:XX:XX:XX:XX:XX, [00..FF];<br><WILDCARD> – -, XX:XX:XX:XX:XX:XX, [00..FF]. , 0, MAC-, . |
| 9 | MAC- , ( ). | **wlc-30(config-acl-rule)# match destination-mac <ADDR><WILDCARD>** | |
| 10 | TCP/UDP- , ( ). | **wlc-30(config-acl-rule)# match source-port { <PORT> \| any }** | <PORT> – TCP/UDP- , [1..65535]. «any» TCP/UDP- . |
| 11 | TCP/UDP- , ( ). | **wlc-30(config-acl-rule)# match destination-port { <PORT> \| any }** | |
| 12 | 802.1p , ( ). | **wlc-30(config-acl-rule)# match os <COS>** | <COS> – 802.1p , [0..7]. |
| 13 | DSCP, ( ). IP Precedence. | **wlc-30(config-acl-rule)# match dscp <DSCP>** | <DSCP> – DSCP, [0..63]. |
| 14 | IP Precedence, ( ). DSCP. | **wlc-30(config-acl-rule)# match ip-precedence <IPP>** | <IPP> – IP Precedence, [0..7]. |
| 15 | VLAN, ( ). | **wlc-30(config-acl-rule)# match vlan <VID>** | <VID> – VLAN, [1..4094]. |
| 16 | . | **wlc-30(config-acl-rule)# enable** | |
| 17 | . | **wlc-30(config-if-gi)# service-acl input <NAME>** | <NAME> – , 31 . |

QoS.

:

192.168.20.0/24.

:

:

```
wlc-30# configure
wlc-30(config)# ip access-list extended white
wlc-30(config-acl)# rule 1
wlc-30(config-acl-rule)# action permit
wlc-30(config-acl-rule)# match source-address 192.168.20.0 255.255.255.0
wlc-30(config-acl-rule)# enable
wlc-30(config-acl-rule)# exit
wlc-30(config-acl)# exit
```

gi1/0/19 :

```
wlc-30(config)# interface gigabitethernet 1/0/19
wlc-30(config-if-gi)# service-acl input white
```

:

```
wlc-30# show ip access-list white
```

# IPS/IDS

IPS/IDS (*Intrusion Prevention System / Intrusion Detection System*) — — , .

. IPS/IDS . . CLI .

EmergingThreats, .

| | | | |
|---|---|---|---|
| 1 | IPS/IDS. | **wlc-30(config)# security ips policy <NAME>** | <NAME> – , 32 |
| 2 | ( ). | **wlc-30(config-ips-policy)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 3 | IP-, IPS/IDS. | **wlc-30(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 32 . |
| 4 | IP-, IPS/IDS ( ). | **wlc-30(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 32 . |
| 5 | IPS/IDS. | **wlc-30(config)# security ips** | |
| 6 | IPS/IDS. | **wlc-30(config-ips)# policy <NAME>** | <NAME> – , 32 |
| 7 | wlc-30 IPS/IDS ( ). | **wlc-30(config-ips)# perfomance max** | IPS/IDS . |
| 8 | EVE ( ). | **wlc-30(config-ips)# logging storage-path <DEVICE_NAME>** | <DEVICE_NAME> USB- MMC-. |
| 9 | IPS/IDS. | **wlc-30(config-ips )# enable** | |
| 10 | IPS/IDS . | **wlc-30(config-if-gi)# service-ips enable** | |

### IPS/IDS

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config-ips)# auto-upgrade** | |
| 2 | . | **wlc-30(config-ips-auto-upgrade)# user-server <WORD>** | <WORD> – , 32 . |
| 3 | ( ). | **wlc-30(config-ips-upgrade-user-server)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 4 | URL. | **wlc-30(config-ips-upgrade-user-server)# url <URL>** | <URL> – , URL- 8 255 .<br>URL- :<br>• .rule;<br>• classification.config;<br>• , / . |

| | | | |
|---|---|---|---|
| 5 | ( ). | **wlc-30(config-ips-upgrade-user-server)# upgrade interval <HOURS>** | <HOURS> – , 1 240.<br>: 24 . |

IPS/IDS, , — 50 .

, , %STORAGE_IPS_MGR-I-ERR: There no free space in rules directory.
.

| | |
|---|---|
| https://sslbl.abuse.ch/ | SSL Blacklist «» SSL-, .. , . SHA1- SSL-. |
| https://feodotracker.abuse.ch/ | Feodo Tracker – Feodo. Feodo ( Cridex Bugat) ( , /) . ( A, B, C D), . |
| https://rules.emergingthreats.net/open/suricata/rules/botcc.rules | . : Shadowserver.org, Zeus Tracker, Palevo Tracker, Feodo Tracker, Ransomware Tracker. |
| https://rules.emergingthreats.net/open/suricata/rules/ciarmy.rules | www.cinsarmy.com. |
| https://rules.emergingthreats.net/open/suricata/rules/compromised.rules | . : Daniel Gerzo's BruteForceBlocker, The OpenBL, Emerging Threats Sandnet, SidReporter Projects. |
| https://rules.emergingthreats.net/open/suricata/rules/drop.rules | / www.spamhaus.org. |
| https://rules.emergingthreats.net/open/suricata/rules/dshield.rules | www.dshield.org. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-activex.rules | ActiveX-. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-attack_response.rules | , . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-chat.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-current_events.rules | , . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dns.rules | DNS, DNS , DNS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-dos.rules | DOS-. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-exploit.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-ftp.rules | FTP, FTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-games.rules | : World of Warcraft, Starcraft .. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp.rules | ICMP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-icmp_info.rules | ICMP-. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-imap.rules | IMAP, IMAP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-inappropriate.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-info.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-malware.rules | , HTTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-misc.rules | . |

| | |
|---|---|
| https://rules.emergingthreats.net/open/suricata/rules/emerging-mobile_malware.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-netbios.rules | NetBIOS, NetBIOS. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-p2p.rules | P2P- (Bittorrent, Gnutella, Limewire). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-policy.rules | ( MySpace, Ebay). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-poprules | POP3, POP3. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-rpc.rules | RPC, RPC. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scada.rules | SCADA-. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-scan.rules | , (Nessus, Nikto, portscanning). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-shellcode.rules | , - . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-smtp.rules | SMTP, SMTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-sql.rules | SQL. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-telnet.rules | telnet, telnet. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-tftp.rules | TFTP, TFTP. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-trojan.rules | . |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-user_agents.rules | HTTP- ( HTTP- User-Agent). |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-l.rules | VoIP-. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_client.rules | -. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_server.rules | -. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-web_specific_apps.rules | -. |
| https://rules.emergingthreats.net/open/suricata/rules/emerging-worm.rules | . |

## IPS/IDS

:

.

192.168.1.0/24 — .

:

, :

```
wlc-30(config)# object-group network LAN
wlc-30(config-object-group-network)# ip prefix 192.168.1.0/24
wlc-30(config-object-group-network)# exit
```

WLC-30 DNS- IPS/IDS:

```
wlc-30(config)# domain lookup enable
wlc-30(config)# domain name-server 8.8.8.8
```

IPS/IDS:

```
wlc-30(config)# security ips policy OFFICE
wlc-30(config-ips-policy)# description "My Policy"
wlc-30(config-ips-policy)# protect network-group LAN
```

IPS/IDS bridge 1:

```
wlc-30(config)# bridge 1
wlc-30(config-bridge)# service-ips enable
```

IPS/IDS:

```
wlc-30(config)# security ips
wlc-30(config-ips)# logging storage-patch usb://DATA
wlc-30(config-ips)# policy OFFICE
wlc-30(config-ips)# enable
```

, IPS/IDS :

```
wlc-30(config-ips)# perfomance max
```

EmergingThreats.net, etnetera.cz Abuse.ch:

```
wlc-30(config-ips)# auto-upgrade
wlc-30(config-auto-upgrade)# user-server ET-Open
wlc-30(config-ips-upgrade-user-server)# description «emerging threats open rules»
wlc-30(config-ips-upgrade-user-server)# url https://rules.emergingthreats.net/open/suricata-4.0/emerging-all.
rules
wlc-30(config-ips-upgrade-user-server)# exit
wlc-30(config-auto-upgrade)# user-server Aggressive
wlc-30(config-ips-upgrade-user-server)# description «Etnetera aggressive IP blacklist»
wlc-30(config-ips-upgrade-user-server)# url https://security.etnetera.cz/feeds/etn_aggressive.rules
wlc-30(config-ips-upgrade-user-server)# upgrade interval 4
wlc-30(config-ips-upgrade-user-server)# exit
wlc-30(config-auto-upgrade)# user-server SSL-BlackList
```

```
wlc-30(config-ips-upgrade-user-server)# description «Abuse.ch SSL Blacklist»
wlc-30(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslblacklist.rules
wlc-30(config-ips-upgrade-user-server)# upgrade interval 4
wlc-30(config-ips-upgrade-user-server)# exit
wlc-30(config-auto-upgrade)# user-server C2-Botnet
wlc-30(config-ips-upgrade-user-server)# description «Abuse.ch Botnet C2 IP Blacklist»
wlc-30(config-ips-upgrade-user-server)# url https://sslbl.abuse.ch/blacklist/sslipblacklist.rules
wlc-30(config-ips-upgrade-user-server)# upgrade interval 4
wlc-30(config-ips-upgrade-user-server)# exit
```

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config)# security ips-category user-defined <WORD>** | <WORD> – , 32 . |
| 2 | ( ). | **wlc-30(config-ips-category)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |

| | | | |
|---|---|---|---|
| 3 | . | **wlc-30(config-ips-category)# rule <ORDER>** | <ORDER> – , [1..512]. |
| 4 | ( ). | **wlc-30(config-ips-category-rule)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 5 | . | **wlc-30(config-ips-category-rule)# action { alert \| reject \| pass \| drop }** | • alert – , IPS/IDS ;<br>• reject – . TCP TCP-RESET, ICMP-ERROR. IPS/IDS ;<br>• pass – ;<br>• drop – , IPS/IDS . |
| 6 | IP-, . | **wlc-30(config-ips-category-rule)# protocol <PROTOCOL>** | <PROTOCOL> – any/ip/icmp/http/tcp/udp<br><br>«any» |
| 7 | IP- , . | **wlc-30(config-ips-category-rule)# source-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><br><ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32].<br><br><OBJ_GR_NAME> – IP-, IP- , 31 .<br><br>• protect – protect- IPS/IDS;<br>• external – external- IPS/IDS.<br><br>«any» IP- . |
| 8 | TCP/UDP- , .<br><br>protocol icmp, source-port any. | **wlc-30(config-ips-category-rule)# source-port {any \| <PORT> \| object-group <OBJ-GR-NAME> }** | <PORT> – TCP/UDP- , [1..65535].<br><br><OBJ_GR_NAME> – TCP/UDP- , 31 .<br><br>«any» TCP/UDP- . |
| 9 | IP- , . | **wlc-30(config-ips-category-rule)# destination-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><br><ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32].<br><br><OBJ_GR_NAME> – IP-, IP- , 31 .<br><br>• protect – , protect IPS/IDS;<br>• external - , external IPS/IDS.<br><br>«any» IP- . |
| 10 | TCP/UDP- , .<br><br>protocol icmp, destination-port any. | **wlc-30(config-ips-category-rule)# destination-port {any \| <PORT> \| object-group <OBJ-GR-NAME> }** | <PORT> – TCP/UDP- , [1..65535].<br><br><OBJ_GR_NAME> – TCP/UDP- , 31 .<br><br>«any» TCP/UDP- . |
| 11 | , . | **wlc-30(config-ips-category-rule)# direction { one-way \| round-trip }** | • one-way – .<br>• round-trip – . |
| 12 | , IPS/IDS , . | **wlc-30(config-ips-category-rule)# meta log-message <MESSAGE>** | <MESSAGE> – , 129 . |

| | | | |
|---|---|---|---|
| 13 | , , ( ). | **wlc-30(config-ips-category-rule)# meta classification-type { not-suspicious \| unknown \| bad-unknown \| attempted-recon \| successful-recon-limited \| successful-recon-largescale \| attempted-dos \| successful-dos \| attempted-user \| unsuccessful-user \| successful-user \| attempted-admin \| successful-admin \| rpc-portmap-decode \| shellcode-detect \| string-detect \| suspicious-filename-detect \| suspicious-login \| system-call-detect \| tcp-connection \| trojan-activity \| unusual-client-port-connection \| network-scan \| denial-of-service \| non-standard-protocol \| protocol-command-decode \| web-application-activity \| web-application-attack \| misc-activity \| misc-attack \| icmp-event \| inappropriate-content \| policy-violation \| default-login-attempt }** | • not-suspicious – .<br>• unknown – .<br>• bad-unknown – .<br>• attempted-recon – .<br>• successful-recon-limited – .<br>• successful-recon-largescale – .<br>• attempted-dos – .<br>• successful-dos – .<br>• attempted-user – .<br>• unsuccessful-user – .<br>• successful-user – .<br>• attempted-admin – .<br>• successful-admin – .<br>• rpc-portmap-decode – RPC.<br>• shellcode-detect – .<br>• string-detect – .<br>• suspicious-filename-detect – -.<br>• suspicious-login – .<br>• system-call-detect – .<br>• tcp-connection – TCP-.<br>• trojan-activity – .<br>• unusual-client-port-connection – .<br>• network-scan – .<br>• denial-of-service – .<br>• non-standard-protocol – .<br>• protocol-command-decode – .<br>• web-application-activity – -.<br>• web-application-attack – -.<br>• misc-activity – .<br>• misc-attack – .<br>• icmp-event – ICMP.<br>• inappropriate-content – .<br>• policy-violation – .<br>• default-login-attempt – /. |
| 14 | DSCP, ( ). | **wlc-30(config-ips-category-rule)# ip dscp <DSCP>** | <DSCP> – DSCP, [0..63]. |
| 15 | (TTL), ( ). | **wlc-30(config-ips-category-rule)# ip ttl <TTL>** | <TTL> – TTL, [1..255]. |
| 16 | IP-, ( ).<br>protocol any. | **wlc-30(config-ips-category-rule)# ip protocol-id <ID>** | <ID> – IP-, [1..255]. |
| 17 | ICMP CODE, ( ).<br>protocol icmp. | **wlc-30(config-ips-category-rule)# ip icmp code <CODE>** | <CODE> – CODE ICMP, [0..255]. |
| | | **wlc-30(config-ips-category-rule)# ip icmp code comparison-operator { greater-than \| less-than }** | ip icmp code:<br>• greater-than – ..<br>• less-than – .. |
| 18 | ICMP ID, ( ).<br>protocol icmp. | **wlc-30(config-ips-category-rule)# ip icmp id <ID>** | <ID> – ID ICMP, [0.. 65535]. |
| 19 | ICMP Sequence-ID, ( ).<br>protocol icmp. | **wlc-30(config-ips-category-rule)# ip icmp sequence-id <SEQ-ID>** | <SEQ-ID> – Sequence-ID ICMP, [0.. 4294967295]. |
| 20 | ICMP TYPE, ( ).<br>protocol icmp. | **wlc-30(config-ips-category-rule)# ip icmp type <TYPE>** | <TYPE> – TYPE ICMP, [0..255]. |
| | | **wlc-30(config-ips-category-rule)# ip icmp type comparison-operator { greater-than \| less-than }** | ip icmp type:<br>• greater-than – ..<br>• less-than – .. |
| 21 | TCP Acknowledgment-Number, ( ).<br>protocol tcp. | **wlc-30(config-ips-category-rule)# ip tcp acknowledgment-number <ACK-NUM>** | <ACK-NUM> – Acknowledgment-Number TCP, [0.. 4294967295]. |
| 22 | TCP Sequence-ID, ( ).<br>protocol tcp. | **wlc-30(config-ips-category-rule)# ip tcp sequence-id <SEQ-ID>** | <SEQ-ID> – Sequence-ID TCP, [0.. 4294967295]. |
| 23 | TCP Window-Size, ( ).<br>protocol tcp. | **wlc-30(config-ips-category-rule)# ip tcp window-size <SIZE>** | <SIZE> – Window-Size TCP, [0.. 65535]. |

| | | | |
|---|---|---|---|
| 24 | HTTP, ( ).<br><br>protocol http. | **wlc-30(config-ips-category-rule)# ip http { accept \| accept-enc \| accept-lang \| client-body \| connection \| content-type \| cookie \| file-data \| header \| header-names \| host \| method \| protocol \| referer \| request-line \| response-line \| server-body \| start \| start-code \| start-msg \| uri \| user-agent }** | Suricata 4.X.<br><br>https://suricata.readthedocs.io/en/suricata-4.1.4/rules/http-keywords.html |
| 25 | URI LEN HTTP, ( ).<br><br>protocol http. | **wlc-30(config-ips-category-rule)# ip http urilen <LEN>** | <LEN> – [0.. 65535]. |
| | | **wlc-30(config-ips-category-rule)# ip http urilen comparison-operator { greater-than \| less-than }** | ip http urilen:<br><br>• greater-than – .<br>• less-than – . |
| 26 | (Payload content), ( ). | **wlc-30(config-ips-category-rule)# payload content <CONTENT>** | <CONTENT> – , 1024 . |
| 27 | ( ).<br><br>payload content. | **wlc-30(config-ips-category-rule)# payload no-case** | |
| 28 | ( ).<br><br>payload content. | **wlc-30(config-ips-category-rule)# payload depth <DEPTH>** | <DEPTH> – , [1.. 65535].<br><br>. |
| 29 | ( ).<br><br>payload content. | **wlc-30(config-ips-category-rule)# payload offset <OFFSET>** | <OFFSET> – , [1.. 65535].<br><br>. |
| 30 | , ( ). | **wlc-30(config-ips-category-rule)# payload data-size <SIZE>** | <SIZE> – , [0.. 65535]. |
| | | **wlc-30(config-ips-category-rule)# payload data-size comparison-operator { greater-than \| less-than }** | payload data-size:<br><br>• greater-than – .<br>• less-than – . |
| 31 | , ( ). | **wlc-30(config-ips-category-rule)# threshold count <COUNT>** | <COUNT> – , [1.. 65535]. |
| 32 | ,<br><br>(, threshold count). | **wlc-30(config-ips-category-rule)# threshold second <SECOND>** | <SECOND> – , [1.. 65535]. |
| 33 | .<br><br>(, threshold count). | **wlc-30(config-ips-category-rule)# threshold track { by-src \| by-dst }** | • by-src – IP-.<br>• by-dst – IP-. |
| 34 | . | **wlc-30(config-ips-category-rule)# threshold type {threshold \| limit \| both }** | • threshold – .<br>• limit – <COUNT> <SECOND>.<br>• both – threshold limit.<br><br>, <SECOND> <COUNT> , <SECOND>. |
| 35 | . | **wlc-30(config-ips-category-rule)# enable** | |

:

IP 192.168.1.10 DOS- ICMP- .

:

:

```
wlc-30(config)# security ips-category user-defined USER
```

:

```
wlc-30(config-ips-category)# rule 10
wlc-30(config-ips-category-rule)# description «Big ICMP DoS»
```

:

```
wlc-30(config-ips-category-rule)# action drop
```

:

```
wlc-30(config-ips-category-rule)# meta log-message «Big ICMP DoS»
wlc-30(config-ips-category-rule)# meta classification-type successful-dos
```

:

```
wlc-30(config-ips-category-rule)# protocol icmp
```

icmp, any:

```
wlc-30(config-ips-category-rule)# source-port any
wlc-30(config-ips-category-rule)# destination-port any
```

:

```
wlc-30(config-ips-category-rule)# destination-address ip 192.168.1.10
```

:

```
wlc-30(config-ips-category-rule)# source-address any
```

:

```
wlc-30(config-ips-category-rule)# direction one-way
```

1024 :

```
wlc-30(config-ips-category-rule)# payload data-size 1024
wlc-30(config-ips-category-rule)# payload data-size comparison-operator greate r-than
```

, 3 /, :

```
3 / = 3145728
  1 = 8192
3145728 / 8192 = 384
384 * 60 = 23040
```

```
wlc-30(config-ips-category-rule)# threshold count 23040
wlc-30(config-ips-category-rule)# threshold second 60
wlc-30(config-ips-category-rule)# threshold track by-dst
wlc-30(config-ips-category-rule)# threshold type both
```

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config)# security ips-category user-defined <WORD>** | <WORD> – , 32 . |
| 2 | ( ). | **wlc-30(config-ips-category)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 3 | . | **wlc-30(config-ips-category)# rule-advanced <SID>** | <SID> – , [1.. 4294967295]. |
| 4 | ( ). | **wlc-30(config-ips-category-rule-advanced)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |

| | | | |
|---|---|---|---|
| 5 | . | **wlc-30(config-ips-category-rule-advanced)# rule-text <LINE>** | <CONTENT> – SNORT 2.X / Suricata 4.X, 1024 .<br>⚠ " '. |
| 6 | . | **wlc-30(config-ips-category-rule-advanced)# enable** | |

:

, Slowloris.

:

:

```
wlc-30(config)# security ips-category user-defined ADV
```

:

```
wlc-30(config-ips-category)# rule-advanced 1
wlc-30(config-ips-category-rule-advanced)# description «Slow Loris rule 1»
wlc-30(config-ips-category-rule-advanced)# rule-text "alert tcp any any -> any 80 (msg:'Possible Slowloris
Attack Detected';
flow:to_server,established; content:'X-a|3a|'; distance:0; pcre:'/\d\d\d\d/'; distance:0; content:'|0d 0a|';
sid:10000001;)"
```

, , , :

```
wlc-30(config-ips-category)# rule-advanced 2
wlc-30(config-ips-category-rule-advanced)# description «Slow Loris rule 2»
wlc-30(config-ips-category-rule-advanced)# rule-text «alert tcp $EXTERNAL_NET any -> $HOME_NET $HTTP_PORTS
(msg:'SlowLoris.py DoS attempt'; flow:established,to_server,no_stream; content:'X-a:'; dsize:<15;
detection_filter:track by_dst, count 3, seconds 30; classtype:denial-of-service; sid: 10000002; rev:1; )
```

## Eltex Distribution Manager

EDM (Eltex Distribution Manager) — .

« » , « » Kaspersky Security Network Kaspersky SafeStream II, (web, email, P2P, ..). , , -, .

IPS , Kaspersky SafeStream II:

- IP- — IP- , ;
- URL- — URL-, -;
- URL- — URL-, « » . ;
- URL- — URL- ;
- URL- — URL- ;
- — , , ;
- — , ;
- URL- — URL- , ;
- URL- -, , Internet of Things (IoT).

EDM Server, . , WLC-30 . EDM Server .

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30 (config)# content-provider** | |

| | | | |
|---|---|---|---|
| 2 | IP- edm-. | **wlc-30 (config-content-provider)# host address <A.B.C.D \| WORD \| X:X:X:X::X>** | <IP-ADDR> – IP- AAA.BBB.CCC.DDD, [0..255];<br><IPV6-ADDR> – IPv6- RADIUS-, X:X:X:X::X, [0.. FFFF].<br>WORD(1-31) – DNS- . |
| 3 | edm-. | **wlc-30 (config-content-provider)# host port <PORT>** | <PORT> – TCP/UDP- , [1..65535]. |
| 4 | . | **wlc-30 (config-content-provider)# storage-device <DEVICE>** | <DEVICE> – usb://Partion_name:/<br>mmc://Partion_name:/ |
| 5 | . | **wlc-30 (config-content-provider)# reboot immediately \| [time <HH:MM:SS>]** | .<br>time <HH:MM:SS> – , WLC-30 <::>. |
| 6 | . | **enable** | |
| 7 | edm- . | **wlc-30 (config-content-provider)# upgrade interval <1-240>** | |
| 8 | ( ). | **wlc-30 (config-content-provider)# description edm** | LINE (1-255) String describing server |
| 9 | IP-, . | **wlc-30 (config)# object-group network <WORD>wlc-30 (config-object-group-network)# ip prefix <ADDR/LEN>** | <WORD> – , 32 .<br><ADDR/LEN> – , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32]. |
| 10 | service-ips. | **wlc-30 (config)# interface gigabitethernet 1/0/Xwlc-30 (config-if-gi)# service-ips enable** | |
| 11 | IPS/IDS. | **wlc-30 (config)# security ips policy WORD(1-31)** | WORD(1-31) |
| 12 | IP-, IPS /IDS. | **wlc-30(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 32 . |
| 13 | . | **wlc-30 (config-ips-policy)# vendor kaspersky** | |
| 14 | . | **wlc-30 (config-ips-vendor)# category WORD(1-64)** | Phishing URL Data Feed – Phishing URL<br>Malicious URL Data Feed – Malicious URL<br>Botnet C&C URL Data Feed – Botnet C&C URL<br>Malicious Hash Data Feed – Malicious Hashes<br>Mobile Malicious Hash Data Feed – Malicious Hashes<br>IP Reputation Data Feed – IP-<br>Mobile Botnet Data Feed – Botnet<br>Ransomware URL Data Feed – Ransomware URL<br>Botnet C&C URL Exact Data Feed – Botnet C&C URL Exact<br>Phishing URL Exact Data Feed – Phishing URL Exact<br>Malicious URL Exact Data Feed – Malicious URL Exact<br>Iot URL Data Feed – IoT URL |
| 15 | . | **wlc-30 (config-ips-vendor-category)# rules action <ACTION>** | <ACTION> - drop \| reject \| alert \| pass - , .<br>• alert – , IPS/IDS ;<br>• reject – . TCP TCP-RESET, ICMP-ERROR. IPS/IDS ;<br>• pass – ;<br>• drop – , IPS/IDS . |
| 16 | . | **wlc-30 (config-ips-vendor-category)# rules count <number>** | <number> |
| 17 | . | **enable** | |
| 18 | IPS/IDS. | **wlc-30 (config)# security ips** | |
| 19 | IPS/IDS. | **wlc-30(config-ips)# policy <NAME>** | <NAME> – , 32 . |
| 20 | wlc-30 IPS /IDS ( ). | **wlc-30(config-ips)# perfomance max** | |
| 21 | USB-, EVE ( ). | **wlc-30(config-ips)# logging storage-path <DEVICE_NAME>** | <DEVICE> - usb://Partion_name:/<br>mmc://Partion_name:/ |
| 22 | IPS/IDS. | **wlc-30(config- ips )# enable** | |

content-provider — ELTEX. content-provider .

```
content-provider
  host address edm.eltex-co.ru
  host port 8098
  upgrade interval 1
  storage-device mmc://TEST:/
  reboot immediately
  enable
exit
```

, IPS.

IP-, IPS/IDS:

```
object-group network objectgroup0
  ip prefix 192.168.30.0/24
exit
```

IPS:

```
interface gigabitethernet 1/0/1
  service-ips enable
exit
```

:

```
security ips policy policy0
  protect network-group objectgroup0
  vendor kaspersky
    category MaliciousURLsDF
      rules action alert
      rules count 100
      enable
    exit
    category MobileBotnetCAndCDF
      rules action alert
      rules count 1000
      enable
    exit
    category APTIPDF
      rules action alert
      rules count 1000
      enable
    exit
```

```
    category APTURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category BotnetCAndCURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category IPReputationDF
      rules action alert
      rules count 1000
      enable
    exit
    category IoTURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category MaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category MobileMaliciousHashDF
      rules action alert
      rules count 1
      enable
    exit
    category PSMSTrojanDF
      rules action alert
      rules count 1
      enable
    exit
    category PhishingURLsDF
      rules action alert
      rules count 1000
      enable
    exit
    category RansomwareURLsDF
      rules action alert
      rules count 1000
      enable
    exit
  exit
exit
```

IPS- :

```
security ips
  performance max
  policy policy0
  enable
exit
```

IPS/IDS :

**show security ips content-provider**:

```
wlc-30# show security ips content-provider
 Server: content-provider
                Last MD5 of received files:        c60bd0f10716d3f48e18f24828337135
                Next update: 30 October 2020 00:37:06
```

- EDM ( md5) .

**show security ips counters**:

```
wlc-30# show security ips counters
TCP flows processed :     191
Alerts generated :        0
Blocked by ips engine :   7
Accepted by ips engine :  51483
```

IPS/IDS , , IPS/IDS.

HTTP- . . . HTTPS- https://ksn-vt.kaspersky-labs.com.

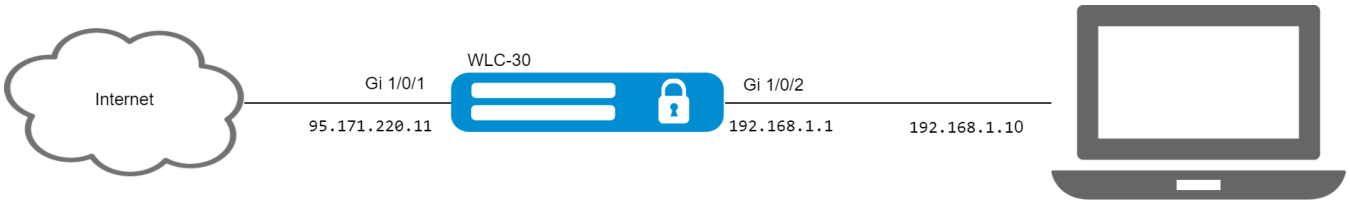
(IPS) IPS.

| | | | |
|---|---|---|---|
| 1 | IP- DNS-, DNS-. | **wlc-30(config)# domain name-server <IP>** | <IP> – IP- DNS-, AAA.BBB.CCC.DDD, [0..255]. |
| 2 | DNS- . | **wlc-30(config)# domain lookup enable** | |
| 3 | IPS/IDS. | **wlc-30(config)# security ips policy <NAME>** | <NAME> – , 32 . |
| 4 | ( ). | **wlc-30(config-ips-policy)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 5 | IP-, . | **wlc-30 (config)# object-group network <WORD>**<br>**wlc-30 (config-object-group-network)# ip prefix <ADDR/LEN>** | <WORD> – , 32 .<br><ADDR/LEN> – , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] EE [1..32]. |
| 6 | IP-, IPS /IDS. | **wlc-30(config-ips-policy)# protect network-group <OBJ-GROUP-NETWORK_NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 32 . |
| 7 | IP-, IPS /IDS ( ). | **wlc-30(config-ips-policy)# external network-group <OBJ-GROUP-NETWORK_NAME>** | <OBJ-GROUP-NETWORK-NAME> – IP-, 32 . |
| 8 | . | **wlc-30(config)# object-group content-filter <NAME>** | <NAME> – , 31 . |
| 9 | ( ). | **wlc-30(config-object-group-content-filter)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 10 | . | **wlc-30(config-object-group-content-filter)# vendor <CONTENT-FILTER-VENDOR>** | <CONTENT-FILTER-VENDOR> – . . |
| 11 | . | **wlc-30(config-object-group-cf-kaspersky)# category <CATEGORY>** | <CATEGORY> – . . |
| 12 | IPS/IDS. | **wlc-30(config)# security ips** | |
| 13 | IPS/IDS. | **wlc-30(config-ips)# policy <NAME>** | <NAME> – , 32 . |
| 14 | wlc-30 IPS /IDS ( ). | **wlc-30(config-ips)# perfomance max** | IPS/IDS . |
| 15 | EVE ( ). | **wlc-30(config-ips)# logging storage-path <DEVICE_NAME>** | <DEVICE_NAME> – USB- MMC-. |
| 16 | IPS/IDS. | **wlc-30(config-ips )# enable** | |
| 17 | IPS/IDS . | **wlc-30(config-if-gi)# service-ips enable** | |
| 18 | . | **wlc-30(config)# security ips-category user-defined <WORD>** | <WORD> – , 32 . |
| 19 | ( ). | **wlc-30(config-ips-category)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 20 | . | **wlc-30(config-ips-category)# rule <ORDER>** | <ORDER> – , [1..512]. |
| 21 | ( ). | **wlc-30(config-ips-category-rule)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 22 | . | **wlc-30(config-ips-category-rule)# action { alert \| reject \| pass \| drop }** | • alert – , IPS/IDS ;<br>• reject – . TCP- TCP-RESET, ICMP-ERROR. IPS/IDS ;<br>• pass – ;<br>• drop – , IPS/IDS . |
| 23 | IP-, HTTP. | **wlc-30(config-ips-category-rule)# protocol http** | |

| | | | |
|---|---|---|---|
| 24 | IP- , . | **wlc-30(config-ips-category-rule)# source-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><br><ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32].<br><br><OBJ_GR_NAME> – IP-, IP- , 31 .<br><br>• protect – , protect IPS/IDS;<br>• external – , external IPS/IDS.<br><br>«any» IP- . |
| 25 | TCP- , . | **wlc-30(config-ips-category-rule)# source-port {any \| <PORT> \| object-group <OBJ-GR-NAME> }** | <PORT> – TCP/UDP- , [1..65535].<br><br><OBJ_GR_NAME> – TCP/UDP- , 31 .<br><br>«any» TCP/UDP- . |
| 26 | IP- , . | **wlc-30(config-ips-category-rule)# destination-address {ip <ADDR> \| ip-prefix <ADDR/LEN> \| object-group <OBJ_GR_NAME> \| policy-object-group { protect \| external } \| any }** | <ADDR> – IP- , AAA.BBB.CCC.DDD, [0..255];<br><br><ADDR/LEN> – IP- , AAA.BBB.CCC.DDD/EE, AAA – DDD [0..255] LEN [1..32].<br><br><OBJ_GR_NAME> – IP-, IP- , 31 .<br><br>• protect – , protect IPS/IDS;<br>• external - , external IPS/IDS.<br><br>«any» IP- . |
| 27 | TCP- , .<br><br>http TCP 80.<br><br>web- . | **wlc-30(config-ips-category-rule)# destination-port {any \| <PORT> \| object-group <OBJ-GR-NAME> }** | <PORT> – TCP/UDP- , [1..65535].<br><br><OBJ_GR_NAME> – TCP/UDP- , 31 .<br><br>«any» TCP/UDP- . |
| 28 | , . | **wlc-30(config-ips-category-rule)# direction { one-way \| round-trip }** | • one-way – .<br>• round-trip – . |
| 29 | IPS/IDS , . | **wlc-30(config-ips-category-rule)# meta log-message <MESSAGE>** | <MESSAGE> – , 129 . |
| 30 | . | **wlc-30(config-ips-category-rule)# ip http content-filter <NAME>** | <NAME> – 31 .<br><br>any – http- . |
| 31 | . | **wlc-30(config-ips-category-rule)# enable** | |

:

http-, adult-content, casino, online-betting, online-lotteries 192.168.1.0/24




:

firewall.

, :

```
wlc-30(config)# object-group network LAN
wlc-30(config-object-group-network)# ip prefix 192.168.1.0/24
wlc-30(config-object-group-network)# exit
```

DNS- IPS/IDS:

```
wlc-30(config)# domain lookup enable
wlc-30(config)# domain name-server 8.8.8.8
```

IPS/IDS:

```
wlc-30(config)# security ips policy OFFICE
wlc-30(config-ips-policy)# description "My Policy"
wlc-30(config-ips-policy)# protect network-group LAN
```

IPS/IDS gigabitethernet 1/0/2:

```
wlc-30(config)# interface gigabitethernet 1/0/2
wlc-30(config-if-gi)# service-ips enable
```

IPS/IDS:

```
wlc-30(config)# security ips
wlc-30(config-ips)# logging storage-path usb://DATA
wlc-30(config-ips)# policy OFFICE
wlc-30(config-ips)# enable
```

, IPS/IDS :

```
wlc-30(config-ips)# perfomance max
```

:

```
wlc-30(config)# object-group content-filter Black
wlc-30(config-object-group-content-filter)# vendor kaspersky-lab
wlc-30(config-object-group-cf-kaspersky)# category adult-content
wlc-30(config-object-group-cf-kaspersky)# category casino
wlc-30(config-object-group-cf-kaspersky)# category online-betting
wlc-30(config-object-group-cf-kaspersky)# category online-lotteries
```

:

```
wlc-30(config)# security ips-category user-defined USER
```

:

```
wlc-30(config-ips-category)# rule 10
wlc-30(config-ips-category-rule)# description «Content-Filter Block»
```

:

```
wlc-30(config-ips-category-rule)# action drop
```

:

```
wlc-30(config-ips-category-rule)# meta log-message «Corporate policy violation»
```

:

```
wlc-30(config-ips-category-rule)# protocol http
```

http- TCP- , any:

```
wlc-30(config-ips-category-rule)# source-port any
```

TCP- http 80 , - , any:

```
wlc-30(config-ips-category-rule)# destination-port any
```

:

```
wlc-30(config-ips-category-rule)# destination-address any
```

:

```
wlc-30(config-ips-category-rule)# source-address policy-object-group protect
```

:

```
wlc-30(config-ips-category-rule)# direction one-way
```

Black:

```
wlc-30(config-ips-category-rule)# ip http content-filter Black
```

:

```
wlc-30(config-ips-category-rule)# enable
wlc-30(config-ips-category-rule)# exit
wlc-30(config-ips-category-rule)# threshold type both
```

""

, - — , (, ..).

«» — . WLC-30 «» , Mail Proxy.

, , «» :

- - SPF;
- , DKIM;
- DMARC;
- MX- , ;
- ;
- RBL;
- SMTP- SMTP-;
- Unicode, ;
- .

, , .

⚠ «» , .

**1) MX- , , IP- WLC-30 «».**

**2) SMTP Proxy, Proxy WLC-30 «».**

| | | | |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | . | **wlc-30(config)# hostname <NAME>** | <NAME> – 64 . |
| 2 | . | **wlc-30(config)# domain name <NAME>** | <NAME> – 255 . |
| 3 | IP- DNS-, DNS-. | **wlc-30(config)# domain name-server <IP>** | <IP> – AAA.BBB.CCC.DDD, 0 255. |
| 4 | DNS. | **wlc-30(config)# domain lookup enable** | |
| 5 | «» | **wlc-30(config)# security antispam profile <NAME>** | <NAME> – 31 . |
| 6 | «» (). | **wlc-30(config-antispam-profile)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 7 | , «» «». | **wlc-30(config-antispam-profile)# mark-type <MARK-TYPE>** | <MARK-TYPE> – , «». :<br>– header – X-Spam ;<br>– subject – [SPAM] . |
| 8 | (). | **wlc-30(config)# object-group email <NAME>** | <NAME> – 31 . |
| 9 | (). | **wlc-30(config-object-group-email)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 10 | (). | **wlc-30(config-object-group-email)# email <NAME>** | <NAME> – 63 . |
| 11 | «» (). | **wlc-30(config-antispam-profile)# rule <ORDER>** | <ORDER> – , 1 100. |
| 12 | «» (). | **wlc-30(config-antispam-profile)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 13 | IP- , ( ). | **wlc-30(config-antispam-profile-rule)# sender ip <NAME>** | <NAME> – 31 . |
| 14 | , ( ). | **wlc-30(config-antispam-profile-rule)# sender email <NAME>** | <NAME> – 31 . |
| 15 | . | **wlc-30(config-antispam-profile-rule)# action <ACTION>** | <ACTION> – . :<br>– reject – , . |
| 16 | «» (). | **wlc-30(config-antispam-profile-rule)# enable** | |
| 17 | . | **wlc-30(config)# mailserver domain <DOMAIN-NAME>** | <DOMAIN-NAME> – 31 . |
| 18 | (). | **wlc-30(config-mailserver-domain)# description <DESCRIPTION>** | <DESCRIPTION> – 255 . |
| 19 | . | **wlc-30(config-mailserver-domain)# mail domain <NAME>** | <NAME> – 63 . |
| 20 | IP- , «» WLC-30 SMTP Proxy. | **wlc-30(config-mailserver-domain)# mail server ip <ADDR>** | <ADDR> – AAA.BBB.CCC.DDD, 0 255. |
| 21 | «», . | **wlc-30(config-mailserver-domain)# profile antispam <NAME>** | <NAME> – 63 . |
| 22 | . | **wlc-30(config-mailserver-domain)# enable** | |
| 23 | . | **wlc-30(config)# mailserver** | |
| 24 | . | **wlc-30(config-mailserver)# domain <NAME>** | <NAME> – 63 . |
| 25 | TLS (). | **wlc-30(config-mailserver)# tls keyfile <TYPE> <NAME>** | <TYPE> – . :<br>• ca – ;<br>• server-key – ;<br>• server-crt – ;<br>• dh – -.<br><NAME> – , 31 . |
| 26 | TLS (). TLS , . | **wlc-30(config-mailserver)# tls enable** | |
| 27 | (). | **wlc-30(config-mailserver)# headers max-size <SIZE>** | <SIZE> – , 50 200. |
| 28 | (). | **wlc-30(config-mailserver)# mail max-size <SIZE>** | <SIZE> – , 5120 51200. |
| 29 | SMTP- HELO EHLO SMTP- (). | **wlc-30(config-mailserver)# smtp helo-required** | |
| 30 | SMTP VRFY SMTP- (). | **wlc-30(config-mailserver)# smtp vrfy-enable** | |
| 31 | . | **wlc-30(config-mailserver)# enable** | |

:

WLC-30 «» SMTP Proxy , , eltex-co.ru.


:

, MX- eltex-co.ru IP- WLC-30:

```
wlc-30@eltex:~$ dig +noall +answer eltex-co.ru MX
eltex-co.ru.        3548        IN        MX        10 mail-gate.eltex-co.ru.
wlc-30@eltex:~$ dig +noall +answer mail-gate.eltex-co.ru A
mail-gate.eltex-co.ru. 3453        IN        A        95.171.220.11
```

:

```
wlc-30# config
wlc-30(config)# interface gi1/0/1
wlc-30(config-if-gi)# ip address 95.171.220.11/18
wlc-30(config-if-gi)# ip firewall disable
wlc-30(config-if-gi)# exit
wlc-30(config)# interface gi1/0/2
wlc-30(config-if-te)# ip address 192.168.1.1/24
wlc-30(config-if-te)# ip firewall disable
wlc-30(config-if-te)# exit
```

, DNS. FQDN (. Fully Qualified Domain Name — ), MX eltex-co.ru:

```
wlc-30(config)# hostname mail-gate
wlc-30(config)# domain name eltex-co.ru
wlc-30(config)# domain name-server 1.1.1.1
wlc-30(config)# domain lookup enable
```

«», X-Spam , :

```
wlc-30(config)# security antispam profile SimpleProfile
wlc-30(config-antispam-profile)# description "Basic Antispam profile without rules"
wlc-30(config-antispam-profile)# mark-type header
wlc-30(config-antispam-profile)# exit
```

, eltex-co.ru . «», :

```
wlc-30(config)# mailserver domain MainDomain
wlc-30(config-mailserver-domain)# mail domain eltex-co.ru
wlc-30(config-mailserver-domain)# description "Mail domain eltex-co.ru"
wlc-30(config-mailserver-domain)# mail server ip 192.168.1.10
wlc-30(config-mailserver-domain)# profile antispam SimpleProfile
wlc-30(config-mailserver-domain)# enable
wlc-30(config-mailserver-domain)# exit
```

TLS:

```
wlc-30(config)# mailserver
wlc-30(config-mailserver)# domain MainDomain
wlc-30(config-mailserver)# tls keyfile ca ca.crt
wlc-30(config-mailserver)# tls keyfile server-crt server.crt
wlc-30(config-mailserver)# tls keyfile server-key server.key
wlc-30(config-mailserver)# tls enable
wlc-30(config-mailserver)# enable
wlc-30(config-mailserver)# exit
```

.

**firewall SMTP (TCP 25).**