



Continent Enterprise Firewall Version 4

NBAD

Administrator guide



© **SECURITY CODE LLC, 2023. All rights reserved.**

All rights to operation manuals are reserved.

This document is shipped along with the product kit. It is covered by all terms of license agreement. You may not copy this document in printed or electronic form, in whole or part, or deliver it to third parties on commercial purpose without a special written consent of Security Code LLC.

Security Code LLC reserves the right to change the information contained herein without special notice.

Mailing address:	115230, Russian Federation, Moscow, 1st Nagatinsky proezd 10/1
Phone:	+7 (495) 982-30-20
E-mail:	info@securitycode.ru
Web:	www.securitycode.ru

Table of contents

Introduction	4
List of abbreviations	5
Overview	6
Purpose and main functions	6
Run the Configuration Manager	7
Configuration and use	9
Activate NBAD	9
Configure NBAD	10
View and delete blocked IP addresses	12
Documentation	13

Introduction

This manual is designed for administrators of Continent Enterprise Firewall, Version 4 (hereinafter — Continent). It contains information about the purpose and the core functions of the Continent NBAD.

This document contains links to documents [1]–[7].

Website. Information about SECURITY CODE LLC products can be found on <https://www.securitycode.ru>.

Technical support. You can contact technical support by phone: +7 800 505 30 20 or by email: support@securitycode.ru.

Training. You can learn more about hardware and software products of SECURITY CODE LLC in authorized education centers. The list of the centers and information about learning environment can be found on <https://www.securitycode.ru/company/education/training-courses/>.

You can contact a company's representative for more information about trainings by email: education@securitycode.ru.

Version 4.1.7 — Released on December 5th, 2023.

List of abbreviations

DNS	Domain Name System
DoS	Denial of Service
FIN	Final
ICMP	Internet Control Message Protocol
IP	Internet Protocol
UTM	Unified Threat Management

Overview

Purpose and main functions

The Network Behavior Anomaly Detector (NBAD) is a self-learning component that identifies and prevents scanning, protocol validation and DoS attacks. The component's operation algorithm is based on network traffic analysis techniques which take changes in traffic properties over time into account.

Attention!

The learning process is performed only on SYN-scan, SYN-flood and FIN/RST-flood templates.

The NBAD supports the following attack patterns:

Attack type	Pattern description	Note
SYN-scan	Detection pattern for a port scanning attack by sending SYN packets from a single IP address	
ICMP-scan	Detection pattern for ICMP-scan by setting the threshold number of the ICMP ECHO REQUEST packets from a single IP address	
UDP-scan	Detection pattern for ICMP PORT UNREACHABLE packets sent with the set threshold number of UDP connections from the sender's IP address	
Null Payload ICMP packet	Detection pattern for null payload ICMP packets (contain only headers)	
DNS max length	Detection pattern for DNS max length	
Packet Sanity	Detection pattern for a packet sanity check (TCP flags, non-zero ports)	
Small Packet MTU	Detection pattern for DoS attacks by sending large amounts of data using small packets. Because of high latency, the packets consume server resources	
DNS-spoofing	Detection pattern for MITM attacks (man in the middle) where the attacker alters domain name cache data so that the fake IP address returns	
DNS-mismatch	Detection pattern for different DNS responses to a single DNS request within a set period of time	
DNS-reply mismatch	Detection pattern for DNS responses with an incorrect request identifier or a port within a set period of time	
SYN-flood	Detection pattern for DoS attacks by sending an exceeding number of SYN packets from a single IP address to a targeted system within a set period of time	
SMURF-attack	Detection pattern for a fake broadcast ping request that uses the victim's source IP address. All hosts respond to this request	The sources of the attack are not tracked, blocking is not performed
FIN/RST-flood	Detection pattern for DoS attacks by sending an exceeding number of FIN or RST packets from a single IP to a targeted system address within a set period of time	
FRAGGLE-attack	Attack detection pattern similar to SMURF, but for fake broadcast UDP packets	The sources of the attack are not tracked, blocking is not performed
LAND-attack	Attack detection pattern for SYN packets where the addresses of a recipient and a sender match	The sources of the attack are not tracked, blocking is not performed

The NBAD analyzes both internal and external traffic as well as VPN tunnel traffic after its decryption.

If an attack is detected, the NBAD performs one of the following actions:

- registers the event in the network security log and temporarily blocks the attack source;
- registers the event in the network security log;
- collects statistical data.

The NBAD operates in **Learning by time** mode. Learning is performed only on SYN-scan, SYN-flood and FIN/RST-flood templates. Administrator specifies a time period for the component to work in learning mode. At first, the NBAD works with template values. As the learning process is finished, the NBAD uses the data it gained

during the learning process. **Learning by time** mode is enabled for every new IP address in the network. For attacks for which **Learning by time** mode does not work, templates specified by the administrator are used. If the administrator has not configured it, the default settings are used.

Events related to the NBAD as a Security Gateway component are registered in the system log. Events related to changes in the configuration of the Security Gateway or the NBAD are registered in the management log.

Note.

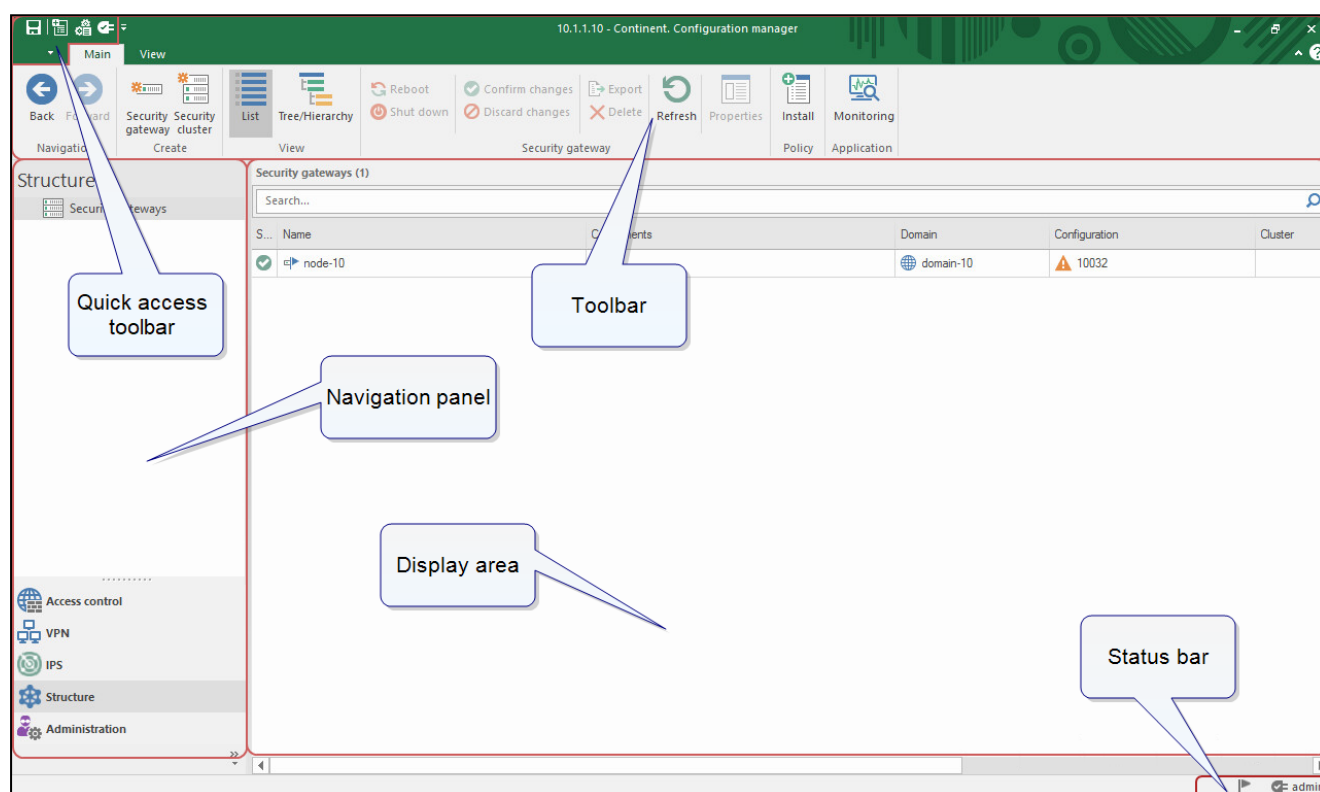
The NBAD works only when the Security Gateway is in UTM mode.

Run the Configuration Manager

To run the Configuration Manager:


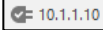
- In the Windows start menu, go to **All apps**, select **Security Code**, then select **Configuration Manager**, or double-click the Configuration Manager shortcut on the Windows desktop.

The Configuration Manager window appears.



The Configuration Manager window contains the following:

Interface element	Description
Toolbar	<p>Contains a set of tools and two tabs:</p> <ul style="list-style-type: none"> Main — displays the toolbar; View — allows to configure the interface of the Configuration Manager. <p>Tools are functional buttons designed to execute frequently used commands. A set of tools depends on a section which you can select in the navigation panel. Operating conditions determine which buttons are displayed and available. When you move the pointer over a button, a tooltip appears</p>
Quick Access Toolbar	<p>Allows quick access to the most frequently used buttons. Contains the following:</p> <ul style="list-style-type: none"> — save current configuration; — install a security policy; — configure the Security Management Server connections; — connect to the Security Management Server; — configure Quick Access Toolbar;

Interface element	Description
Navigation panel	<p>Contains the following sections:</p> <ul style="list-style-type: none"> • Access control — to manage firewall and NAT rules; • VPN — to create and configure VPN; • IPS — to configure IPS settings; • Structure — to manage Security Gateway settings; • Administration — to manage service functions (operations with certificates, backups, licenses, updates, etc.)
Display area	Displays information according to the selected section of the navigation panel
Status bar	<p>Contains the following:</p> <ul style="list-style-type: none"> • the number of tasks currently being executed and the button to open the notification center  where you can find the link to the general task list; • an icon that indicates the status of the connection to the Security Management Server (if there is a connection, this icon also displays the Security Management Server IP address, for example )

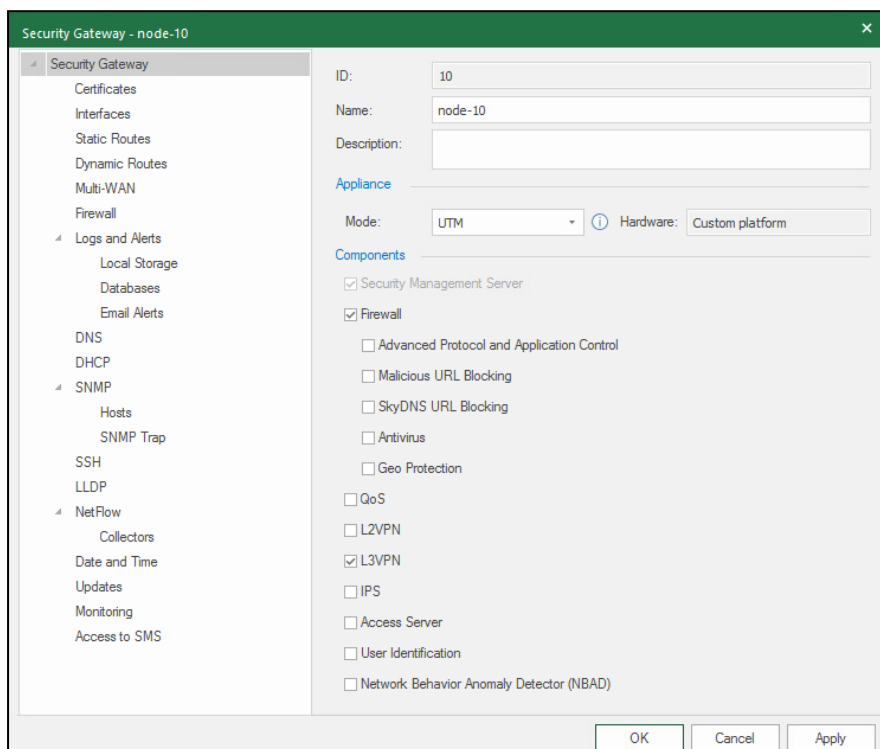
Configuration and use

Activate NBAD

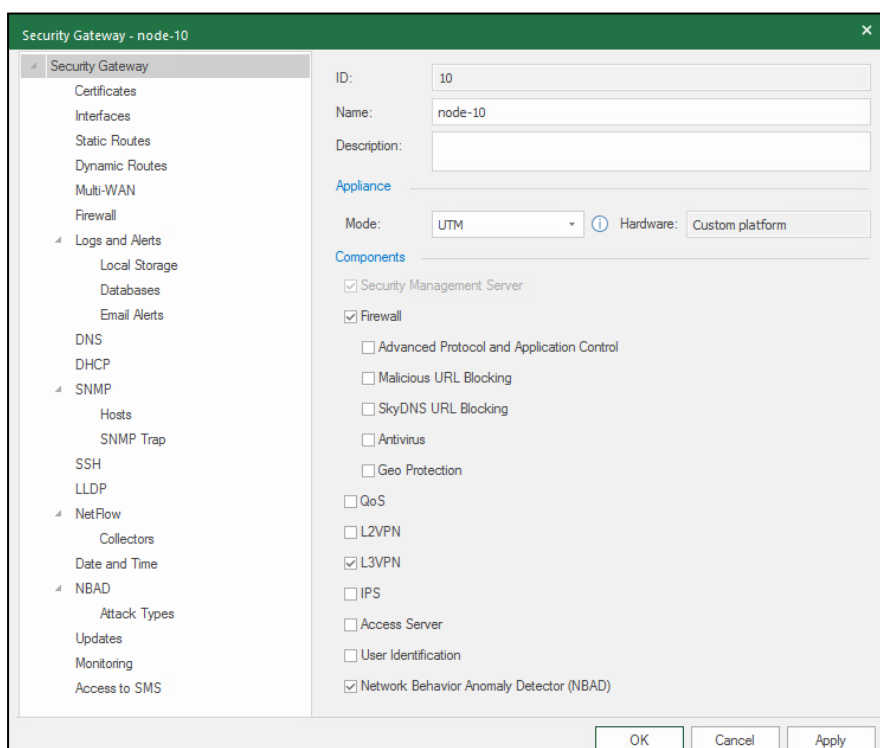
Before you activate the NBAD, make sure the Security Gateway is in UTM mode.


To activate the NBAD:



1. Go to the Security Gateway properties in **UTM** mode.



2. In the list of components, select **Network Behavior Anomaly Detector (NBAD)**. The respective menu item appears on the left.



The NBAD will be activated. In the **Components** column of the **Structure** subsection, the  icon appears.

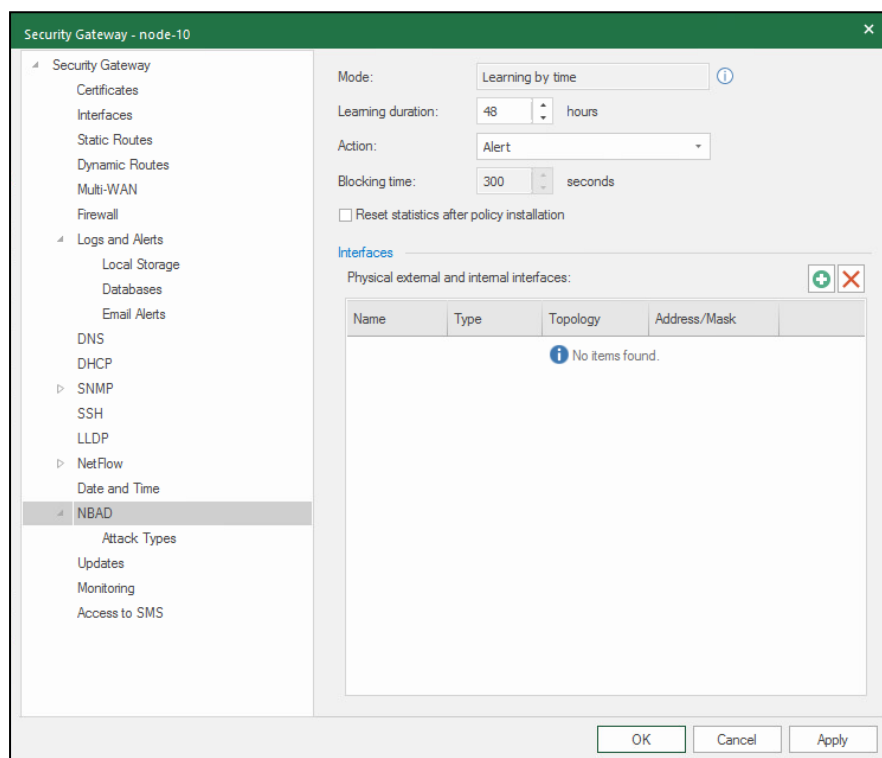
Security gateways (4)							
Search...							
Status	Name	Components	Domain	Configuration	Cluster	Certificate validity, days	Description
Online	node-10		domain-10	10082	-	363	For headquarters
Online	SG-1		domain-10	10082		364	For headquarters

Configure NBAD

To configure NBAD:

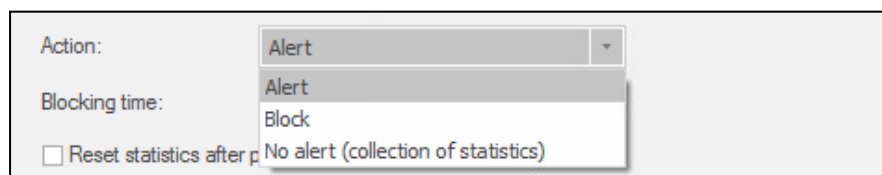
1. On the left, click **NBAD**.

The NBAD parameters appear on the right as in the figure below.



The window is divided into two areas: the settings area and the **Interfaces** area.

2. Set **Learning duration** if necessary.
3. In the **Action** drop-down list, select the reaction to the attack event.




If the **Block** option is selected, the **Blocking time** parameter becomes available for editing.

4. Set the **Blocking time** if necessary.

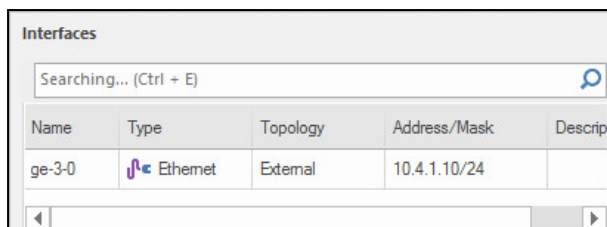
If an attack is detected, the source IP address will be blocked for the specified time.

5. Select **Reset statistics after policy installation** check box if necessary.

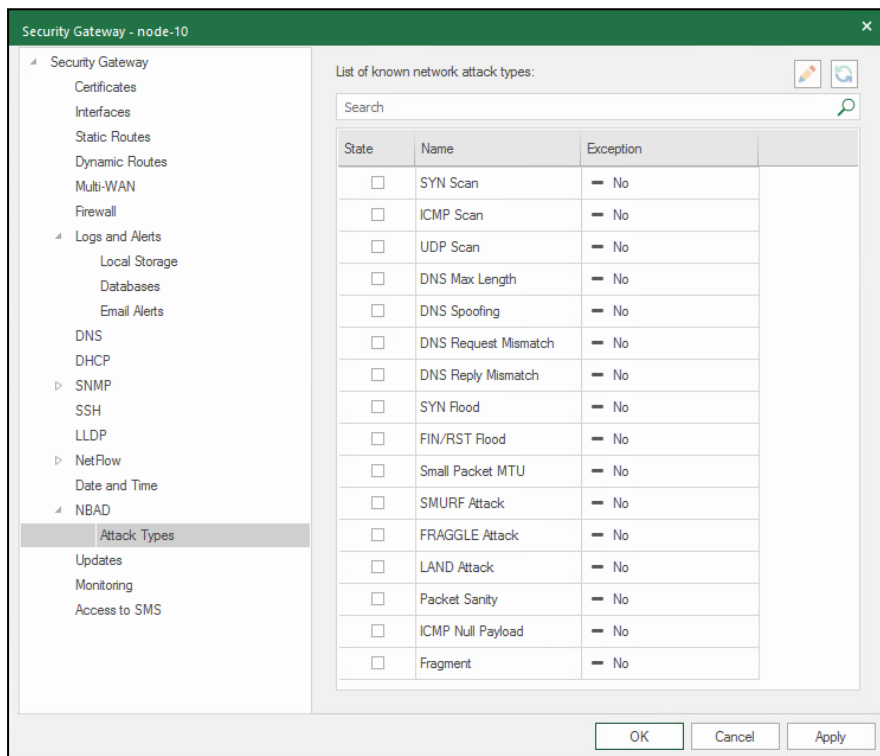
The statistics will be reset when the policy is installed. The NBAD will start working with the values of templates specified in the settings, restarting the learning process.

6. Specify internal and external interfaces required to be analyzed by the NBAD by clicking .

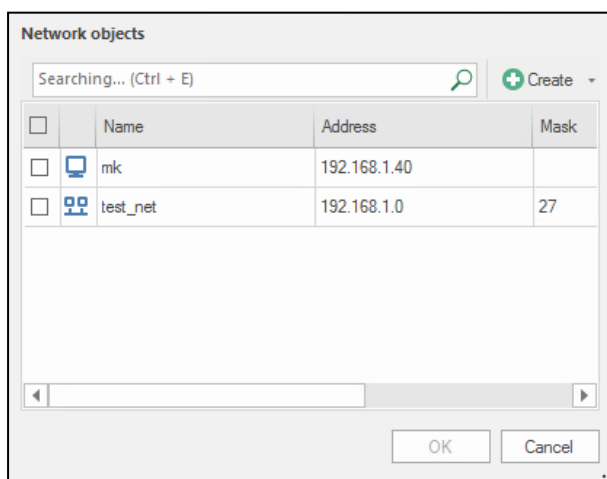
The list of available interfaces appears:



7. Select an interface.
It appears in the respective table.
8. To delete an interface, select it in the table and click
9. Click **Apply**.
10. On the left, select **Attack Types**.



11. Select the attack types in the **State** column that you need the NBAD to track. If necessary, you can exclude a network or host from processing by the module for a specific attack pattern.
12. To configure an exception for an attack pattern, move the pointer over the **Exception** cell and click .
The list of network objects appears:



13. Select the required network objects and click **OK**.

If necessary, you can open the dialog box for creating a new network object in this window.

14. In the Security Gateway dialog box, click **OK**.

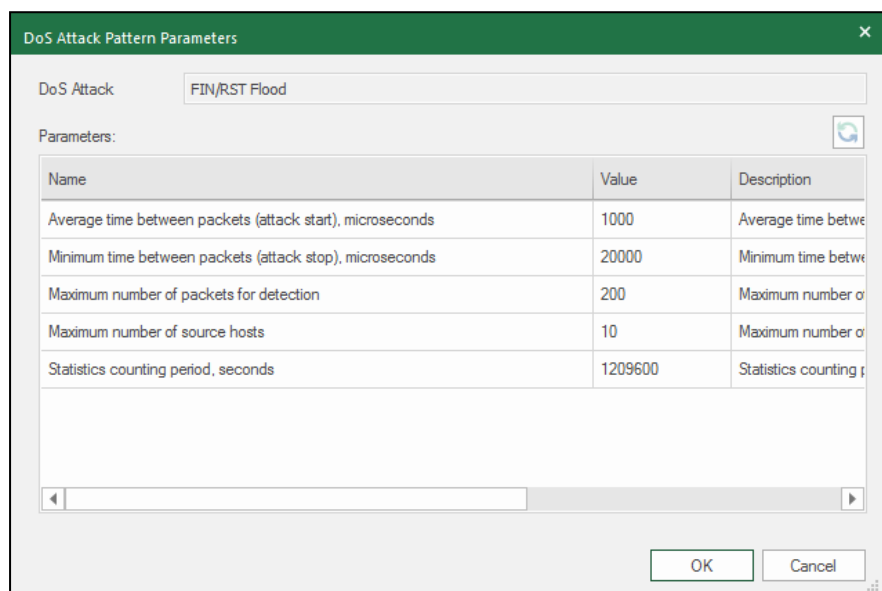
15. Install the policy on the Security Gateway.

You are allowed to edit parameter values in the attack patterns (except **ICMP Null Payload**, **Packet Sanity**, **LAND Attack** and **Fragment** attack patterns).

To edit an attack pattern:

1. Select the required attack pattern double-click its row or click .

The **DoS Attack Pattern Parameters** dialog box appears.



The dialog box titled "DoS Attack Pattern Parameters" has a green header bar. Below the header, there is a tab labeled "DoS Attack" and a text field containing "FIN/RST Flood". Under the "Parameters:" label, there is a table with three columns: "Name", "Value", and "Description". The table contains five rows of parameters. At the bottom right of the dialog, there are "OK" and "Cancel" buttons. A small circular icon with a refresh symbol is located to the right of the "Parameters:" label.

Name	Value	Description
Average time between packets (attack start), microseconds	1000	Average time between packets (attack start), microseconds
Minimum time between packets (attack stop), microseconds	20000	Minimum time between packets (attack stop), microseconds
Maximum number of packets for detection	200	Maximum number of packets for detection
Maximum number of source hosts	10	Maximum number of source hosts
Statistics counting period, seconds	1209600	Statistics counting period, seconds

2. Specify the required parameter values and click **OK**.

Note.

To restore the default values, click , then click **OK**.

View and delete blocked IP addresses

To view and delete blocked IP addresses:

1. In the Security Gateway local menu, go to **Tools | Diagnostics | Command line**.
2. Run the required command in the command line:
 - To view all ipset lists, run the **ipset list** command.
 - To view the list of IP addresses blocked by the NBAD, run the **ipset list RS_dos_protect** command.
 - To delete an IP address, run the **RS_dos_protect <IP address>** command.
 - To clear the list of IP addresses blocked by the NBAD, run the **flush RS_dos_protect** command.

Documentation

1. Continent Enterprise Firewall. Version 4. Administrator guide. Basics.
2. Continent Enterprise Firewall. Version 4. Administrator guide. Deployment.
3. Continent Enterprise Firewall. Version 4. Administrator guide. Firewall.
4. Continent Enterprise Firewall. Version 4. Administrator guide. Intrusion Prevention System.
5. Continent Enterprise Firewall. Version 4. Administrator guide. Management.
6. Continent Enterprise Firewall. Version 4. Administrator guide. VPN.
7. Continent Enterprise Firewall. Version 4. Administrator guide. Networking functions.