

УТВЕРЖДЕНО

ВУ.РТНК.00001-04.1 34 01-13-ЛУ

**Программно-аппаратный комплекс
«Шлюз безопасности Bel VPN Gate 4.1»**

РУКОВОДСТВО ОПЕРАТОРА

Руководство администратора

Мониторинг

ВУ.РТНК.00001-04.1 34 01-13

Листов 20

Инд. № подл.	Подп. и дата	Взам. инд. №	Инв. № дубл.	Подп. и дата

Содержание

Мониторинг	3
Выдача статистики.....	4
Настройка SNMP-агента для выдачи статистики	4
Трап-сообщения.....	18
Настройка SNMP-агента для отправления трапов	18

Мониторинг

Мониторинг шлюза безопасности Bel VPN Gate 4.1 осуществляется по протоколу обмена SNMP. SNMP-менеджер имеет возможность только запрашивать содержимое базы данных агента. Настройка SNMP-агента для выдачи статистики и база данных MIB, которую он поддерживает, описана в разделе «Выдача статистики».

SNMP-агент может посылать SNMP-менеджеру сообщение о возникшем событии в виде трап-сообщения. Настройка SNMP-агента для посылки трап-сообщений и список этих сообщений описаны в разделе «Трап-сообщения».

В качестве SNMP-менеджера для шлюза безопасности Bel VPN Gate 4.1 может быть использована:

- бесплатная утилита NET-SNMP (<http://www.net-snmp.org/>), которая является простейшим SNMP-менеджером. При работе с SNMP-агентом нужно указывать версию SNMP –v 1 или –v 2с.

Выдача статистики

SNMP-менеджер инициирует запрос, который посылает SNMP-агенту для получения значений одной или нескольких переменных. SNMP-агент, отвечая на запрос, возвращает значения запрашиваемых переменных.

Настройка SNMP-агента для выдачи статистики

Cisco-like конфигурация

В интерфейсе командной строки для настройки SNMP-агента по выдаче информации по протоколу SNMP используются команды:

snmp-server community – задает строку, которая играет роль пароля при аутентификации сообщений SNMP и разрешает SNMP-менеджеру чтение статистики из базы управления SNMP-агента

snmp-server location – содержит информацию о физическом расположении SNMP-агента

snmp-server contact – указывается лицо, ответственное за работу SNMP-агента.

Эти команды подробно описаны в документе «Шлюз безопасности Bel VPN Gate 4.1. Cisco-like команды» ([Console_command_reference.pdf](#)).

LSP (native) конфигурация

В конфигурационном файле задание настроек SNMP-агента осуществляется **структурой SNMPPollSettings**. В этой структуре указывается IP-адрес и порт, на который можно получать запросы от SNMP-менеджера, строку, играющую роль пароля при аутентификации сообщений, размещение SNMP-агента и контактное лицо.

Подробно структура SNMPPollSettings описана в документе «Шлюз безопасности Bel VPN Gate 4.1. Создание конфигурационного файла» ([LSP_reference_guide.pdf](#)).

База данных MIB, поддерживаемая SNMP-агентом, разделена на группы. В приведенной ниже таблице (

Таблица 1) перечислены переменные из стандартной группы system, глобальной статистики IKE и IPsec и другие, которые могут быть запрошены SNMP-менеджером.



Note

При принудительном перезапуске сервиса IKE-статистика сбрасывается и начинает считаться со старта Агента. IPsec-статистика считается со старта компьютера и при принудительном перезапуске сервиса не сбрасывается.

В IKE-статистике при подсчете трафика учитывается только количество байт в ISAKMP-пакете. У Cisco же в IKE-статистике учитываются данные из IP-заголовка, UDP-заголовка и Ethernet-заголовка пакета.

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
Статистика по стандартной группе System и специфичным константным значениям				
sysDescr	1.3.6.1.2.1.1.1.0	DisplayString	Текстовое описание сетевого объекта. Строка вида "S-Terra Gate 4.1.<build>"	RFC1213-MIB
sysObjectID	1.3.6.1.2.1.1.2.0	OID	Идентификатор фирмы-производителя (внутри поддерева 1.3.6.1.4.1): 1.3.6.1.4.1.9.1.576(cisco2811 из CISCO-PRODUCTS-MIB)	RFC1213-MIB
sysUpTime	1.3.6.1.2.1.1.3.0	TimeTicks	The time (in hundredths of a second) since the network management portion of the system was last re-initialized. Время в сотых долях секунды с момента последней загрузки системы	RFC1213-MIB
sysContact	1.3.6.1.2.1.1.4.0	DisplayString	Имя контактной персоны и способ контакта.	RFC1213-MIB
sysName	1.3.6.1.2.1.1.5.0	DisplayString	Полное имя домена <hostname>.<domain-name>	RFC1213-MIB
sysLocation	1.3.6.1.2.1.1.6.0	DisplayString	Физическое местоположение агента	RFC1213-MIB
sysServices	1.3.6.1.2.1.1.7.0	int32	Значение, которое характеризует сервисы, предоставляемые узлом. Это значение есть сумма номеров уровней модели OSI в зависимости от того, какие сервисы поддерживаются: 0x01 (физический), 0x02 (канальный), 0x04 (сетевой), 0x08 (точка-точка), 0x40 (прикладной). Например, если поддерживается IP уровень (маршрутизация) и транспортный уровень (точка-точка), то значение sysServices есть сумма 4 и 8. 78 (с2611XM)	RFC1213-MIB
chassisType	1.3.6.1.4.1.9.3.6.1.0	int32	413 (с2811)	OLD-CISCO-CHASSIS-MIB
cipSecMibLevel	1.3.6.1.4.1.9.9.171.1.1.1.0	int32	The level of the IPsec MIB 1	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
snmpSetSerialNo	1.3.6.1.6.3.1.1.6.1.0	int32	<p><An advisory lock used to allow several cooperating SNMPv2 entities, all acting in a manager role, to coordinate their use of the SNMPv2 set operation.</p> <p>Используется как значение, которое ограничивает сверху Cisco-specific значения. Фактически является неформальным обозначением конца MIB-а. Служит для предотвращения возможных коллизий при обработке GET-NEXT операций.</p> <p>0</p>	SNMPv2-MIB
ciscoImageString	1.3.6.1.4.1.9.9.25.1.1.1.2.<i>	DisplayString	<p><The string of this entry.> (описание таблицы – <A table provides content information describing the executing IOS image.>).</p> <p>Выдаются данные для агента:</p> <p>1: "CW_BEGIN\$csp-vpn\$"</p> <p>2: "CW_IMAGE\$C2800NM-CSP-VPN\$"</p> <p>3: "CW_FAMILY\$C2800NM\$"</p> <p>4: "CW_FEATURE\$IP FIREWALL PLUS 3DES VPN SSH IPSEC\$"</p> <p>5: "CW_VERSION\$12.4(13a)\$"</p> <p>6: "CW_MEDIA\$RAM\$"</p> <p>7: "CW_SYSDDESCR\$\$-Terra {Gate Server Client} <major>.<minor>.<build>, Emulation of: Cisco IOS Software, 2800 Software (C2800NM-ADVIPSERVICESK9-M), Version 12.4(13a), RELEASE SOFTWARE (fc1)\$"</p> <p>8: "CW_MAGIC\$\$"</p> <p>9: "CW_END\$csp-vpn\$"</p>	CISCO-IMAGE-MIB
dot1dBaseBridgeAddress	1.3.6.1.2.1.17.1.1.0	MacAddress	<p>Используется при взаимодействии с устройствами Cisco.</p> <p>00 00 00 00 00 00</p>	BRIDGE-MIB
dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2.0	int32	<p>The number of ports controlled by this bridging entity. Используется при взаимодействии с устройствами Cisco.</p> <p>0</p>	BRIDGE-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
dot1dBaseType	1.3.6.1.2.1.17.1.3.0	int32 { unknown (1) , transparent-only (2) , sourceroute-only (3) , srt (4) }	Используется при взаимодействии с устройствами Cisco. srt (4)	BRIDGE-MIB
Глобальная IKE-статистика				
cikeGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.2.1.1.0	uint32	<The number of currently active IPsec Phase-1 IKE Tunnels> Все существующие на данный момент активные ISAKMP SA.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.2.1.2.0	uint32	<The total number of previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInOctets	1.3.6.1.4.1.9.9.171.1.2.1.3.0	uint32	<The total number of octets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество байт, принятых в течение всех IKE-сессий с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInPackets	1.3.6.1.4.1.9.9.171.1.2.1.4.0	uint32	<The total number of packets received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, принятых в течение всех IKE-сессий с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInDropPackets	1.3.6.1.4.1.9.9.171.1.2.1.5.0	uint32	<The total number of packets which were dropped during receive processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов, отвергнутых в течение всех IKE-сессий с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2Exchanges	1.3.6.1.4.1.9.9.171.1.2.1.7.0	uint32	<The total number of IPsec Phase-2 exchanges received by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве респондера.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInP2ExchangeInvalids	1.3.6.1.4.1.9.9.171.1.2.1.8.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and	CISCO-IPSEC-

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
			found to be invalid by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, не состоявшихся по причине ошибки обмена.	FLOW-MONITOR-MIB
cikeGlobalInP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.9.0	uint32	<The total number of IPsec Phase-2 exchanges which were received and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий по созданию IPsec соединений, инициированных партнёрами, которые не состоялись по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.2.1.11.0	uint32	<The total number of octets sent by all currently and previously active and IPsec Phase-1 IKE Tunnels> Количество байт, высланных в течение всех IKE-сессий с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.2.1.12.0	uint32	<The total number of packets sent by all currently and previously active and IPsec Phase-1 Tunnels> Количество ISAKMP-пакетов, высланных в течение всех IKE-сессий с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutDropPkts	1.3.6.1.4.1.9.9.171.1.2.1.13.0	uint32	<The total number of packets which were dropped during send processing by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество ISAKMP-пакетов в течение всех IKE-сессий с момента старта Агента, которые были готовы к отсылке, но по каким-то причинам не были отсланы.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2Exchgs	1.3.6.1.4.1.9.9.171.1.2.1.15.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent by all currently and previously active IPsec Phase-1 IKE Tunnels> Количество успешных Quick Modes в качестве инициатора.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalOutP2ExchgInvalids	1.3.6.1.4.1.9.9.171.1.2.1.16.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and found to be invalid by all currently and	CISCO-IPSEC-FLOW-

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
			previously active IPsec Phase-1 Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявших по причине ошибки обмена.	MONITOR-MIB
cikeGlobalOutP2ExchgRejects	1.3.6.1.4.1.9.9.171.1.2.1.17.0	uint32	<The total number of IPsec Phase-2 exchanges which were sent and rejected by all currently and previously active IPsec Phase-1 IKE Tunnels> Общее количество инициированных IKE-сессий по созданию IPsec соединений, не состоявших по причине рассогласования политик безопасности.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnels	1.3.6.1.4.1.9.9.171.1.2.1.19.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated> Количество созданных ISAKMP SA в качестве инициатора (т.е. по инициативе локальной стороны).	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalInitTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.20.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were locally initiated and failed to activate> Количество инициированных сессий по созданию ISAKMP SA, завершившихся неудачей.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalRespTunnelFails	1.3.6.1.4.1.9.9.171.1.2.1.21.0	uint32	<The total number of IPsec Phase-1 IKE Tunnels which were remotely initiated and failed to activate> Количество сессий по созданию ISAKMP SA, инициированных партнёрами, которые завершились неудачей.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalAuthFails	1.3.6.1.4.1.9.9.171.1.2.1.23.0	uint32	<The total number of authentications which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных сессий по созданию ISAKMP SA, в которых не прошла аутентификация.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalDecryptFails	1.3.6.1.4.1.9.9.171.1.2.1.24.0	uint32	<The total number of decryptations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявших по причине ошибки расшифрования пакета.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cikeGlobalHashValidFails	1.3.6.1.4.1.9.9.171.1.2.1.25.0	uint32	<The total number of hash validations which ended in failure by all current and previous IPsec Phase-1 IKE Tunnels> Количество неудачных операций по проверке значения хэш-функции во всех IKE сессиях.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.2.1.26.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-1 IKE Tunnels> Общее количество IKE-сессий, не состоявшихся по причине отсутствия ISAKMP соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Глобальная IPsec-статистика				
cipSecGlobalActiveTunnels	1.3.6.1.4.1.9.9.171.1.3.1.1.0	uint32	<The total number of currently active IPsec Phase-2 Tunnels> Количество существующих на данный момент IPsec соединений. Период обновления всех переменных этого раздела (Глобальная IPsec-статистика) – 1 секунда. Поэтому, после изменения значения переменной в течение 1 секунды на компьютере может выдаваться устаревшее значение.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalPreviousTunnels	1.3.6.1.4.1.9.9.171.1.3.1.2.0	uint32	<The total number of previously active IPsec Phase-2 Tunnels> Количество IPsec SA с момента старта Агента, которые были созданы, но уже не являются активными, либо удалены.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctets	1.3.6.1.4.1.9.9.171.1.3.1.3.0	uint32	<The total number of octets received by all current and previous IPsec Phase-2 Tunnels. This value is accumulated BEFORE determining whether or not the packet should be decompressed. See also cipSecGlobalInOctWraps for the number of times this counter has wrapped> Количество байт, принятых под защитой всех IPsec SA с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.5.0	uint32	<The number of times the global octets received counter (cipSecGlobalInOctets) has wrapped>	CISCO-IPSEC-FLOW-

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
			Количество переполнений счетчика cipSecGlobalInOctets .	MONITOR-MIB
cipSecGlobalInPkts	1.3.6.1.4.1.9.9.171.1.3.1.9.0	uint32	<The total number of packets received by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, принятых под защитой всех IPsec SA с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDrops	1.3.6.1.4.1.9.9.171.1.3.1.10.0	uint32	<The total number of packets dropped during receive processing by all current and previous IPsec Phase-2 Tunnels. This count does NOT include packets dropped due to Anti-Replay processing> Общее количество всех входящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения (Кроме проигнорированных по Anti-Replay).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInReplayDrops	1.3.6.1.4.1.9.9.171.1.3.1.11.0	uint32	<The total number of packets dropped during receive processing due to Anti-Replay processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех входящих пакетов, отвергнутых локальным устройством посредством механизма Anti-Replay, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.13.0	uint32	<The total number of inbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных входящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalInDecrypts	1.3.6.1.4.1.9.9.171.1.3.1.14.0	uint32	<The total number of inbound decryption's performed by all current and previous IPsec Phase-2 Tunnels> То же самое значение, что и cipSecGlobalInPkts . Общее количество входящих пакетов, которые были расшифрованы всеми IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cipSecGlobalInDecryptFails	1.3.6.1.4.1.9.9.171.1.3.1.15.0	uint32	<The total number of inbound decryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество входящих пакетов, которые были неудачно расшифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctets	1.3.6.1.4.1.9.9.171.1.3.1.16.0	uint32	<The total number of octets sent by all current and pre-vious IPsec Phase-2 Tunnels. This value is accumulated AFTER determining whether or not the packet should be compressed. See also cipSecGlobalOutOctWraps for the number of times this counter has wrapped> Количество байт, отосланных под защитой всех IPsec SA с момента старта Агента.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutOctWraps	1.3.6.1.4.1.9.9.171.1.3.1.18.0	uint32	<The number of times the global octets sent counter (cipSecGlobalOutOctets) has wrapped> Количество переполнений счетчика cipSecGlobalOutOctets .	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutPkts	1.3.6.1.4.1.9.9.171.1.3.1.22.0	uint32	<The total number of packets sent by all current and previous IPsec Phase-2 Tunnels> Количество пакетов, отосланных под защитой всех IPsec SA с момента старта Агента	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutDrops	1.3.6.1.4.1.9.9.171.1.3.1.23.0	uint32	<The total number of packets dropped during send processing by all current and previous IPsec Phase-2 Tunnels> Общее количество всех исходящих пакетов, отвергнутых локальным устройством, при задействовании IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutAuthFails	1.3.6.1.4.1.9.9.171.1.3.1.25.0	uint32	<The total number of outbound authentication's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество всех неудачных исходящих аутентификаций по IPsec соединениям.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalOutEncrypts	1.3.6.1.4.1.9.9.171.1.3.1.26.0	uint32	<The total number of outbound encryption's performed by all current and previous IPsec Phase-2 Tunnels>	CISCO-IPSEC-FLOW-MONITOR-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
			Тоже самое значение, что и cipSecGlobalOutPkts . Общее количество исходящих пакетов, которые были зашифрованы всеми IPsec соединениями.	
cipSecGlobalOutEncryptFails	1.3.6.1.4.1.9.9.171.1.3.1.27.0	uint32	<The total number of outbound encryption's which ended in failure by all current and previous IPsec Phase-2 Tunnels> Общее количество исходящих пакетов, которые были неудачно зашифрованы IPsec соединениями.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecGlobalNoSaFails	1.3.6.1.4.1.9.9.171.1.3.1.29.0	uint32	<The total number of non-existent Security Association in failures which occurred during processing of all current and previous IPsec Phase-2 Tunnels> Общее количество обменов, не состоявшихся по причине отсутствия IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
Статистика по сетевым интерфейсам				
ifPhysAddress	1.3.6.1.2.1.2.2.1.6.<ifIndex>	Octet string	<The interface's address at the protocol layer immediately `below' the network layer in the protocol stack. For interfaces which do not have such an address (e.g., a serial line), this object should contain an octet string of zero length.> MAC-адрес данного интерфейса. Индекс для данного значения берется из ipAdEntIfIndex .<ip>	RFC1213-MIB
ifIndex	1.3.6.1.2.1.2.2.1.1.<ifIndex>	int32	<A unique value for each interface. Its value ranges between 1 and the value of ifNumber. The value for each interface must remain constant at least from one re-initialization of the entity's network management system to the next re-initialization> ifIndex – индекс интерфейса, значение лежит в диапазоне между 1 и ifNumber (ifNumber - число сетевых интерфейсов).	RFC1213-MIB
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1.<ip>	IpAddress	<The IP address to which this entry's addressing information pertains.> Собственно сам <ip> (совпадает с индексом значения).	IP-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3.<ip>	IpAddress	<The subnet mask associated with the IP address of this entry. The value of the mask is an IP address with all the network bits set to 1 and all the hosts bits set to 0.> Маска адреса.	IP-MIB
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2.<ip>	int32	<The index value which uniquely identifies the interface to which this entry is applicable. The interface identified by a particular value of this index is the same interface as identified by the same value of RFC 1573's ifIndex.> Индексом переменной является IP-адрес устройства. Значением – индекс интерфейса (в таблице ifTable), который содержит данный адрес. Период обновления всех переменных этого раздела (Статистика по сетевым интерфейсам) – 5 секунд. Поэтому, после изменения значения переменной в течение 5 секунд на компьютере может выдаваться устаревшее значение.	IP-MIB
CPU (загрузка процессора), Memory - статистика				
cpmCPUTotal5sec	1.3.6.1.4.1.9.9.109.1.1.1.1.3.1	uint32 (1..100)	<The overall CPU busy percentage in the last 5 second period. This object obsoletes the busyPer object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5secRev which has the changed range of value (0..100).> Загрузка процессора за последние 5 секунд (в процентах).	CISCO-PROCESS-MIB
cpmCPUTotal5secRev	1.3.6.1.4.1.9.9.109.1.1.1.1.6.1	uint32 (0..100)	<The overall CPU busy percentage in the last 5 second period. This object deprecates the object cpmCPUTotal5sec and increases the value range to (0..100). This object is deprecated by cpmCPUTotalMonInterval> Загрузка процессора за последние 5 секунд. Отличается от cpmCPUTotal5sec допустимыми пределами.	CISCO-PROCESS-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
cpmCPUTotal1min	1.3.6.1.4.1.9.9.109.1.1.1.1.4.1	uint32 (1..100)	<p><The overall CPU busy percentage in the last 1 minute period. This object obsoletes the avgBusy1 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal1minRev which has the changed range of value (0..100).></p> <p>Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1minRev допустимыми пределами.</p>	CISCO-PROCESS-MIB
cpmCPUTotal1minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.7.1	uint32 (0..100)	<p><The overall CPU busy percentage in the last 1 minute period. This object deprecates the object cpmCPUTotal1min and increases the value range to (0..100).></p> <p>Загрузка процессора за последнюю минуту. Отличается от cpmCPUTotal1min допустимыми пределами.</p>	CISCO-PROCESS-MIB
cpmCPUTotal5min	1.3.6.1.4.1.9.9.109.1.1.1.1.5.1	uint32 (1..100)	<p><The overall CPU busy percentage in the last 5 minute period. This object deprecates the avgBusy5 object from the OLD-CISCO-SYSTEM-MIB. This object is deprecated by cpmCPUTotal5minRev which has the changed range of value (0..100).></p> <p>Средняя загрузка процессора за последние 5 минут (в процентах).</p>	CISCO-PROCESS-MIB
cpmCPUTotal5minRev	1.3.6.1.4.1.9.9.109.1.1.1.1.8.1	uint32 (0..100)	<p><The overall CPU busy percentage in the last 5 minute period. This object deprecates the object cpmCPUTotal5min and increases the value range to (0..100).></p> <p>Загрузка процессора за последние 5 минут. Отличается от cpmCPUTotal5min допустимыми пределами.</p>	CISCO-PROCESS-MIB
busyPer	1.3.6.1.4.1.9.2.1.5.6.0	int32 (0..100)	<p><CPU busy percentage in the last 5 second period. Not the last 5 realtime seconds but the last 5 second period in the scheduler.></p> <p>Загрузка процессора за последние 5 секунд. Аналогично cpmCPUTotal5secRev, за исключением типа переменной. Примечание: данное поведение отличается от Cisco IOS – там указанные значения могут различаться. Значение, выдаваемое</p>	OLD-CISCO-CPU-MIB

Название переменной	OID (идентификатор объекта)	Тип переменной	Значение переменной	MIB
			агентом, зависит от ОС и немного отличается по смыслу от обоих значений Cisco IOS.	
ciscoMemoryPoolUsed	1.3.6.1.4.1.9.9.48.1.1.1.5.1	uint32	<p><Indicates the number of bytes from the memory pool that are currently in use by applications on the managed device.></p> <p>Рассматривается как таблица из одного элемента (с индексом 1), которая задает общее количество используемой физической памяти.</p>	CISCO-MEMORY-POOL-MIB
ciscoMemoryPoolFree	1.3.6.1.4.1.9.9.48.1.1.1.6.1	uint32	<p><Indicates the number of bytes from the memory pool that are currently unused on the managed device.</p> <p>Note that the sum of ciscoMemoryPoolUsed and ciscoMemoryPoolFree is the total amount of memory in the pool></p> <p>Общее количество свободной физической памяти.</p>	CISCO-MEMORY-POOL-MIB

Трап-сообщения

SNMP-агент посылает трап-сообщения о произошедших событиях SNMP-менеджеру.

Настройка SNMP-агента для отправления трапов

Cisco-like конфигурация

В cisco-like конфигурации для отсылки трапов задаются команды:

snmp-server enable traps – для включения отсылки SNMP-трапов

snmp-server host – для задания параметров получателя SNMP-трапов

snmp-server trap-source – для указания интерфейса, с которого посылаются SNMP-трапы.

Эти команды подробно описаны в документе «Шлюз безопасности Bel VPN Gate 4.1. Cisco-like команды» ([Console_command_reference.pdf](#)).

LSP (native) конфигурация

В конфигурационном файле задание настроек SNMP-агента для отсылки трап -сообщений осуществляется в структурах ***SNMPTrapSettings*** и ***TrapReceiver***. В этих структурах указывается IP-адрес и порт, на который отсылаются сообщения SNMP-менеджеру, идентификатор и IP-адрес отправителя трап-сообщения, версия SNMP, в которой создаются трап-сообщения.

Подробно эти структуры описаны в документе «Шлюз безопасности Bel VPN Gate 4.1. Создание конфигурационного файла» ([LSP_reference_guide.pdf](#)).

В приведенной ниже таблице (Таблица 2) перечислены реализованные трапы и переменные, которые высылаются SNMP-менеджеру, и описание трапа.

Таблица 2

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cikeSysFailure	1.3.6.1.4.1.9.9.1 71.2 3 1.3.6.1.4.1.9.9.1 71.2.0.3	cikePeerLocalAddr – адрес local peer cikePeerRemoteAddr – адрес remote peer Оба значения – табличные.	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences an internal or system capacity error.> Сигнализация о внутренней ошибке или исчерпаниии ресурсов при обработке IKE.	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeCertCrlFailure	1.3.6.1.4.1.9.9.1 71.2 4 1.3.6.1.4.1.9.9.1 71.2.0.4	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a Certificate or a Certificate Revoke List (CRL) related error.> Ошибка, связанная с сертификатами или CRL.	CISCO-IPSEC-FLOW-MONITOR-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
cikeProtocolFailure	1.3.6.1.4.1.9.9.1 71.2 5 1.3.6.1.4.1.9.9.1 71.2.0.5	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a protocol related error.> Ошибка, связанная с обработкой протокола IKE: Authentication error (в ситуациях, не попадающих под cikeCertCrlFailure)	CISCO-IPSEC-FLOW-MONITOR-MIB
cikeNoSa	1.3.6.1.4.1.9.9.1 71.2 6 1.3.6.1.4.1.9.9.1 71.2.0.6	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the processing for an IPsec Phase-1 IKE Tunnel experiences a non-existent security association error.> Приход IKE-пакетов на несуществующий SA (Invalid cookie).	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecSetUpFailure	1.3.6.1.4.1.9.9.1 71.2 10 1.3.6.1.4.1.9.9.1 71.2.0.10	cikePeerLocalAddr cikePeerRemoteAddr	<This notification is generated when the setup for an IPsec Phase-2 Tunnel fails.> По тем или иным причинам не удалось создать IPsec SA (при существующем IKE SA). <u>Примечание:</u> этот трап отсылается только при появлении ошибки во время проведения IKE-сессии и тем партнером, на котором случилась ошибка. Если создание соединения прекращено по другим причинам – остановка сервиса, перезагрузка LSP, delete payload, получение нотификации о том, что партнер по своей инициативе прекратил создание соединения, timeout и др., то локальное устройство трап не отсылает. В этом состоит отличие нашего агента от IOS, где трапы отсылаются с обоих партнеров при любой неуспешной сессии по созданию IPsec соединения.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStart	1.3.6.1.4.1.9.9.1 71.2 7 1.3.6.1.4.1.9.9.1 71.2.0.7	cipSecTunLifeTime cipSecTunLifeSize Табличные значения	<This notification is generated when an IPsec Phase-2 Tunnel becomes active.> Это трап-сообщение появляется при успешном создании IPsec SA.	CISCO-IPSEC-FLOW-MONITOR-MIB
cipSecTunnelStop	1.3.6.1.4.1.9.9.1 71.2 8 1.3.6.1.4.1.9.9.1 71.2.0.8	cipSecTunActiveTime Табличное значение	<This notification is generated when an IPsec Phase-2 Tunnel becomes inactive.>	CISCO-IPSEC-FLOW-MONITOR-MIB

Название трапа	SNMPv1 Enterprise and Specific Type; SNMPv2 OID	Список переменных	Значение переменной	MIB
			Это трап-сообщение появляется после удаления IPsec SA (по разным причинам).	
cipsTooMany SAs	1.3.6.1.4.1.9.10.62.2 7 1.3.6.1.4.1.9.10.62.2.0.7	cipsMaxSAs – максимальное количество IPsec SAs. Если не существует предела – 0.	<This trap is generated when a new SA is attempted to be setup while the number of currently active SAs equals the maximum configurable. The variables are: cipsMaxSAs> Отказ от создания SA по причине достигнутого максимального количества SA, указанного в лицензии. В переменной прописывается максимальное количество SA из лицензии.	CISCO-CONFIG-MAN-MIB
ciscoConfigManagementEvent	1.3.6.1.4.1.9.9.4.3.2 1 1.3.6.1.4.1.9.9.4.3.2.0.1	ccmHistoryEventCommandSource = { commandLine(1), snmp(2) } ccmHistoryEventConfigSource = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } ccmHistoryEventConfigDestination = { erase(1), commandSource(2), running(3), startup(4), local(5), networkTftp(6), networkRcp(7) } Табличные значения. Индекс – целое число, начинающееся с единицы. Инкрементируется при каждой посылке трапа данного типа.	<Notification of a configuration management event as recorded in ccmHistoryEventTable.> Всегда ccmHistoryEventCommandSource=1 Несколько вариантов: При вызове lsp_mgr show: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=2 <u>Примечание:</u> аналогично реакции Cisco на команду show run При успешной загрузке LSP: ccmHistoryEventConfigSource=2 ccmHistoryEventConfigDestination=3 <u>Примечание:</u> аналогично реакции Cisco на команду configure terminal Для стартовой загрузки LSP надо задать ccmHistoryEventConfigSource = 4 При отгрузке LSP (по разным причинам): ccmHistoryEventConfigSource=1 ccmHistoryEventConfigDestination=3.	CISCO-CONFIG-MAN-MIB