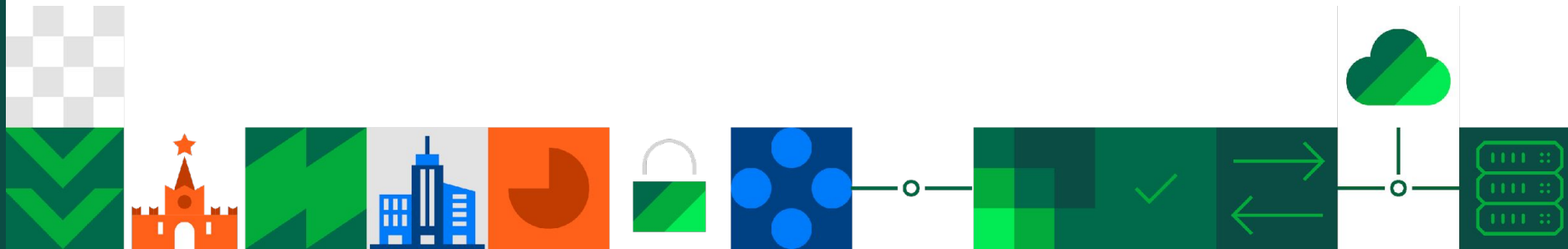


Continent 4





About the product



About the product

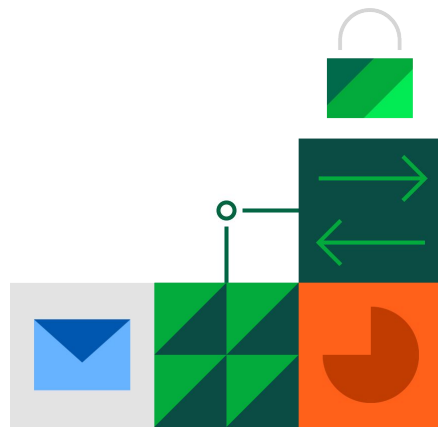


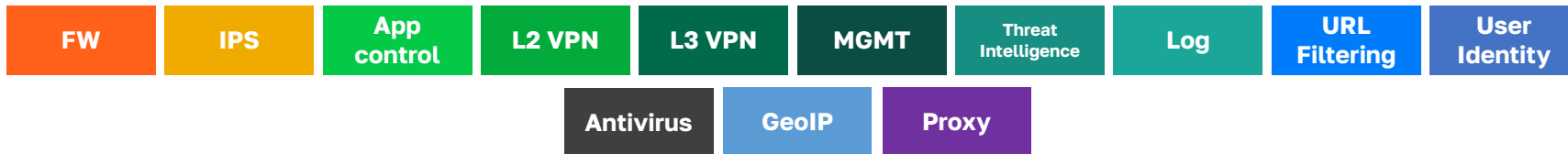
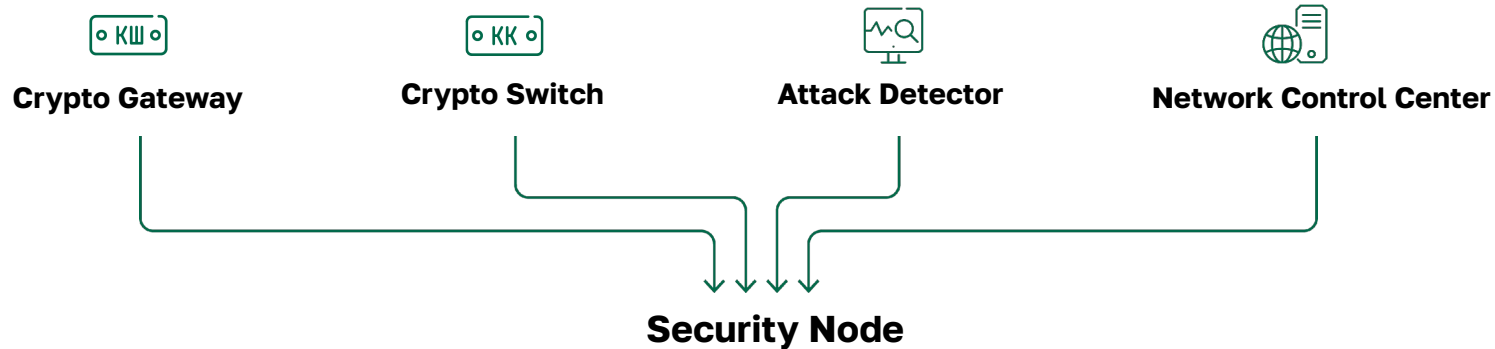
Continent 4

Next Generation Firewall (NGFW)

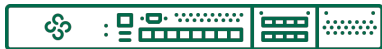
Purpose:

- Centralized protection of the corporate network perimeter
- User access control to the Internet
- Prevention of network intrusions
- Organization of secure remote access





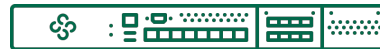
NGFW



Proxy



L2 IDS/IPS



Firewall

Application
Control

URL-filtering

Behavioral Analysis
(based ML)

L3 IDS/IPS

Security

- Application Control (4000+ applications)
- IDPS
- Blocking access to malicious sites (Threat Intelligence)
- URL filtering by categories
- Traffic filtering by country (GeoIP)
- SSL traffic inspection (MiTM)
- Antivirus
- ICAP file submission to third-party sandboxes
- Machine learning-based behavioral analysis



Management

- Centralized infrastructure management via a single console
- LDAP integration
- User authentication portal and identification agent
- Transparent authentication (SSO)
- Flexible monitoring interface
- Management server redundancy



Form Factor

- NGFW/UTM security node
- Layer 2 IDS/IPS
- Dedicated management platform



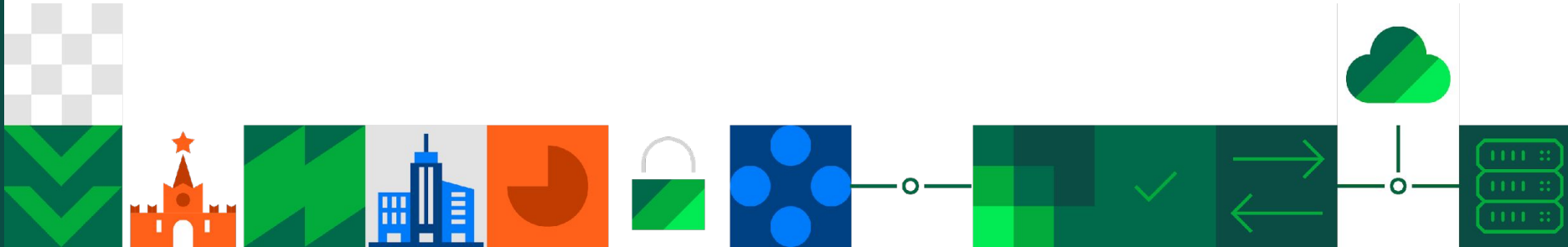
Network Technologies

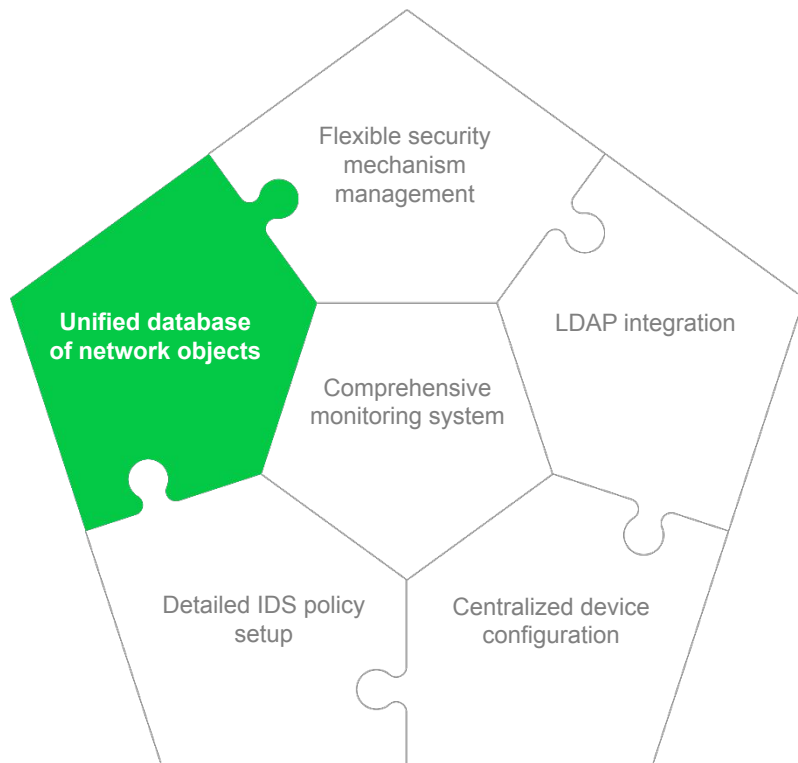
- Dynamic routing
- VRF support
- NAT support
- Proxy server
- Multi-WAN
- QoS
- High-availability clustering with session synchronization





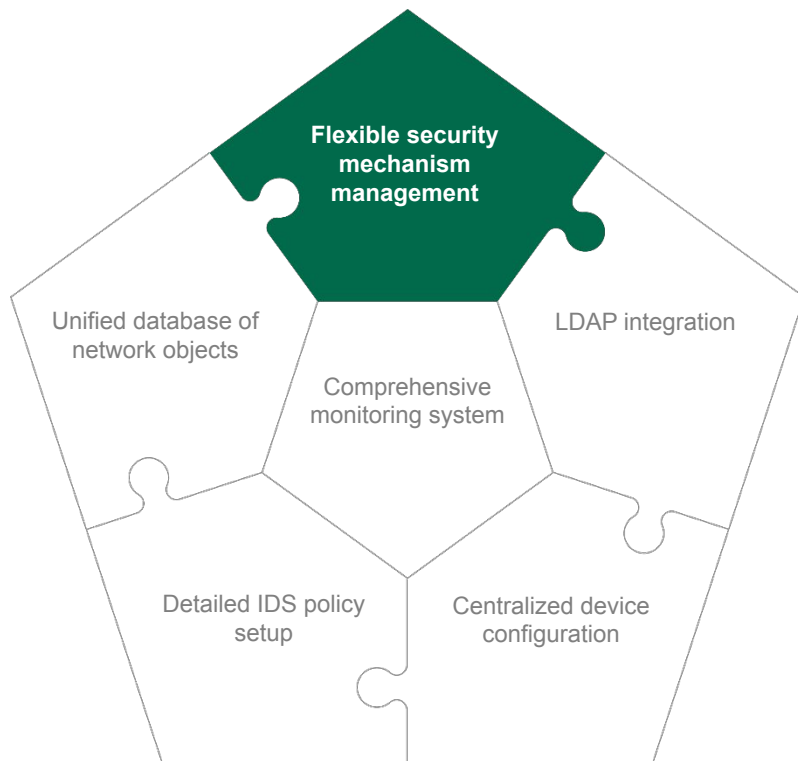
Management System: Continent 4 Network Control Center





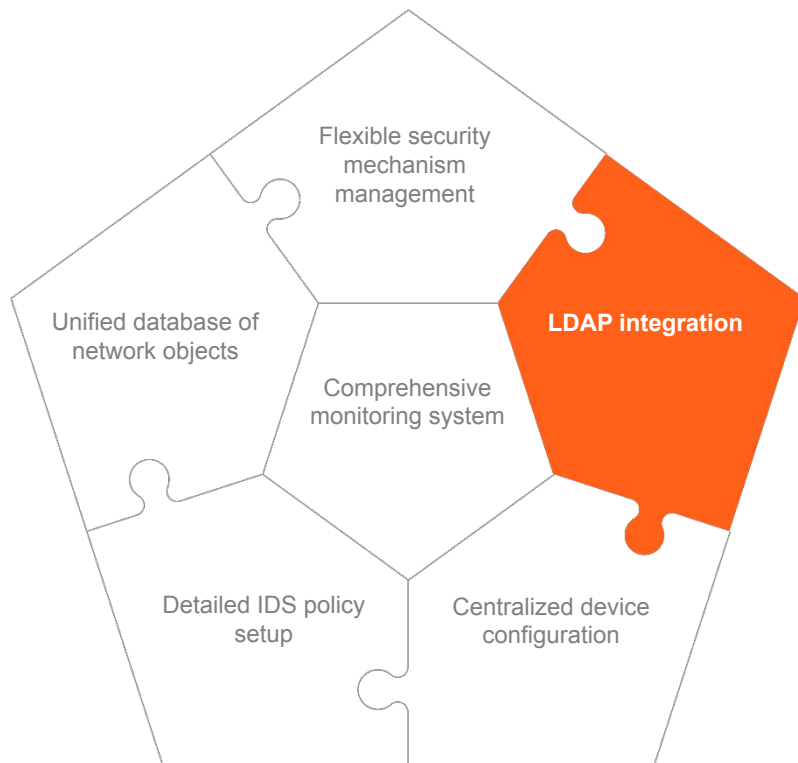
The unified database of network objects is stored in the Control Center (CC). Any object from the CC database can be used in filtering rules. For each rule, specific nodes can be selected for its application. There is support for CC redundancy.

The security administrator will not need to manually configure each node when changes are made to the corporate network.



The traffic distribution system across security mechanisms allows specific modules (such as Application Control, IPS, and URL reputation) to inspect only selected traffic.

This traffic distribution optimizes the device's computational resources and ensures high throughput without compromising the level of security.

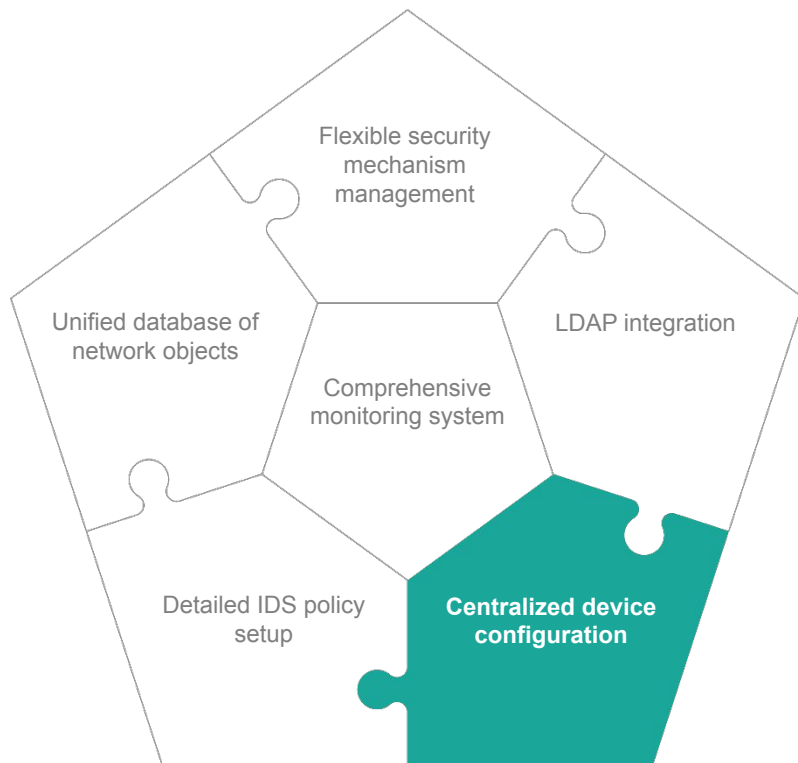


User groups from the shared corporate directory can be added to filtering rules as a source.

Transparent Single Sign-On (SSO) authentication is supported via the Kerberos protocol.

This integration simplifies administration, auditing, and logging processes.

There is no need to create new users locally.

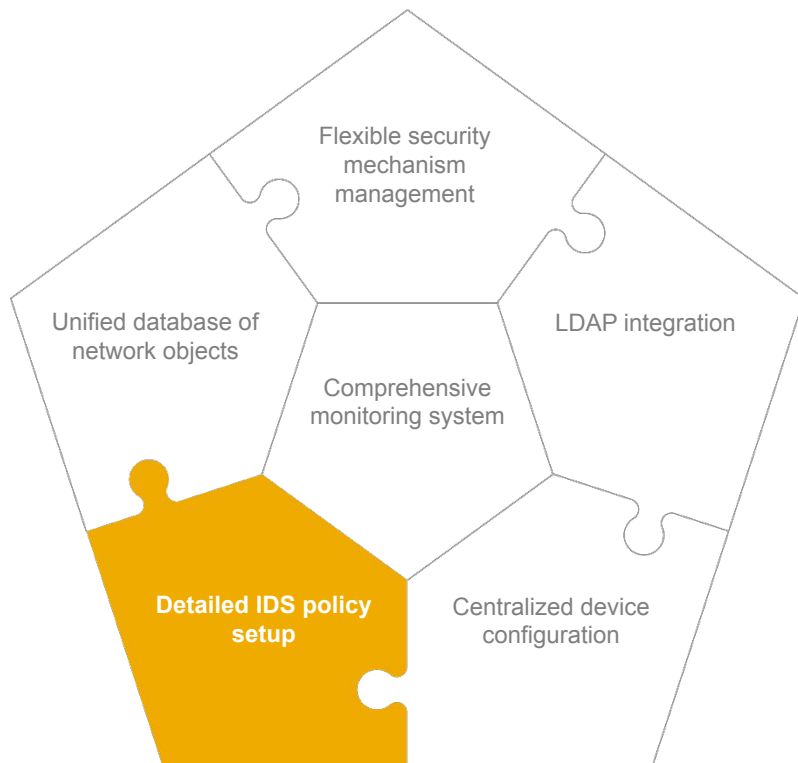


Centralized management of all Continent devices in the network includes their policies, routing rules, and traffic filtering settings.

It supports mass deployment of security nodes, policy import from third-party firewalls, and migration.

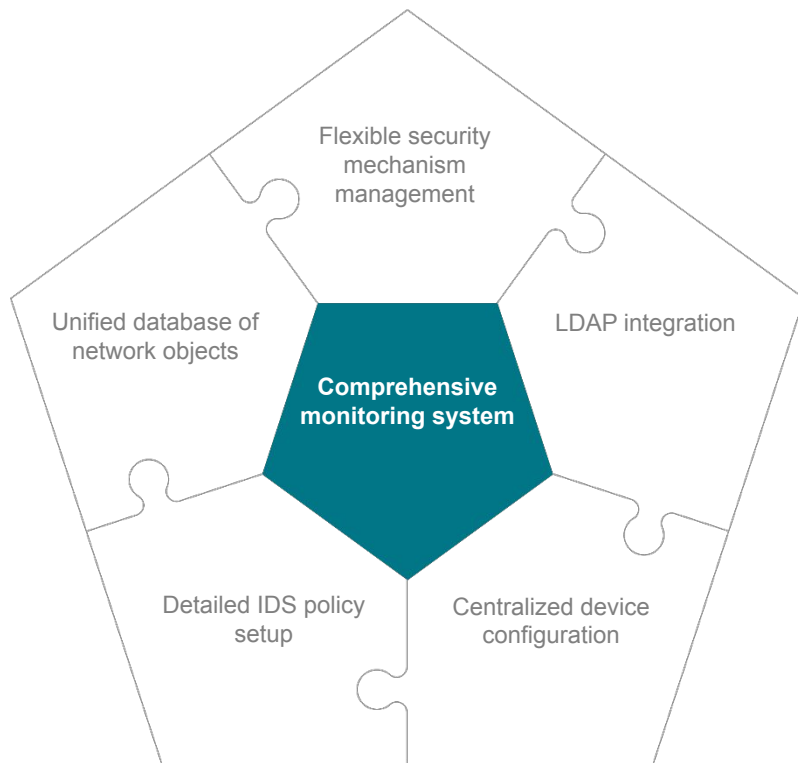
An update scheduler is also available.

Centralized configuration and device management simplify both administration and auditing processes.



Detailed configuration of the IDS system allows traffic to be inspected only based on specified signatures.

The IDS system does not overload the device by processing the entire traffic flow using all signatures, freeing up resources for other security mechanisms and reducing the load on the device.

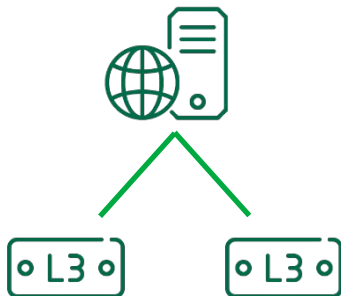


Monitoring is conducted through a web interface independent of the management console.

Logs can be sent to third-party systems for analysis via syslog, NetFlow, and SNMP protocols.

Notifications are received regarding policy installations.

This monitoring system enables quick incident response.



Centralized management

- Network nodes
- Routing settings
- Traffic filtering rules
- VPN communities

User identification and authentication through the local CC database and/or Active Directory using:

- SSO via Kerberos
- Captive portal
- Authentication agents

High-performance event storage and processing system

Real-time event monitoring

Role-based access model for administrators

Multi-factor authentication for remote users:

- Certificates on USB tokens
- Multifactor.ru service
- Avanpost MFA+ platform



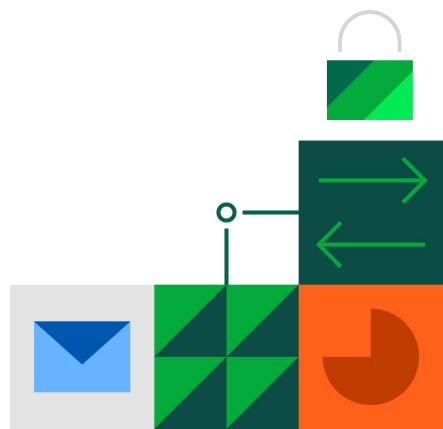
Administrator tasks are automated via API:

- Generation of firewall and NAT rules
- Export of Security Node configurations to external systems
- Export of SN configurations to external Control Centers
- Scheduled policy application
- Scheduled backup creation
- Import of Indicators of Compromise (IoC) from vendors
- Creation of filtering and translation rules based on predefined templates

Automated migration tools support transitions from:

- Check Point
- FortiGate
- Cisco
- Palo Alto
- UserGate
- Continent 3

https://github.com/itseccode/c4_tools



File Main View admin2 ?

Navigation: Back, Forward, Next rule, Previous rule, First rule, Last rule, Import, Section, Expand all, Collapse all, Rule group, Up, Down, Accept, Drop, Copy, Export, Delete, Refresh, Install

Navigation: Sections (3), Rules (7)

Search...

No.	Name	Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	VRF	Install On	De
1		* Any	* Any	DNS	* Any	Accept	* None	Off	Always	None	None	cluster	
2		mgmt	* Any	Continent C...	* Any	Drop	* None	Off	Always	None	None	All	
3		192.168.0.0/24	* Any	ICMP	* Any	Accept	* None	Off	Always	None	None	cluster	
LAN													
WAN													
6		for_cont@cont...	* Any	HTTP	anydesk, pcanywhere, dns, telegram, telegram	Accept	* None	Off	Always	Log	None	cluster	
Internet													
7		for_cont@cont...	* Any	TLS	* Any	Filter	user filter	Off	Always	Log	None	cluster	

Objects

Name	Address	Mask	Description
192.168.0.0/24	192.168.0.0	24	
LAN	192.168.0.0	24	
mgmt	192.168.0.1		
NCC	192.168.0.10		NCC
user1	192.168.0.102		

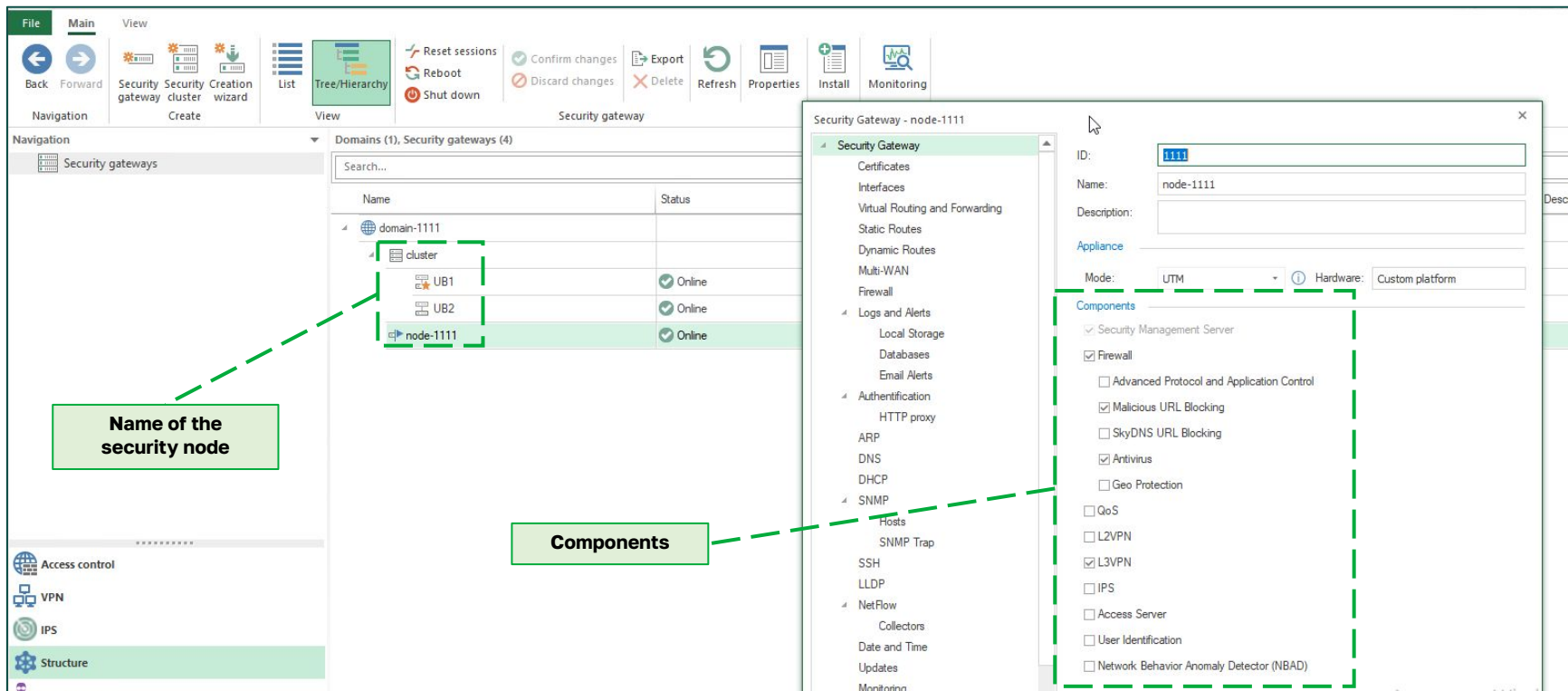
Access control

VPN

IPS

Structure

Administration



The screenshot displays the 'Security gateway' management interface. The main window shows a list of domains and security gateways. A dashed green box highlights the 'node-1111' entry in the list, with a callout box pointing to it containing the text 'Name of the security node'.

The 'Security Gateway - node-1111' configuration window is open, showing various settings. A dashed green box highlights the 'Components' section, with a callout box pointing to it containing the text 'Components'.

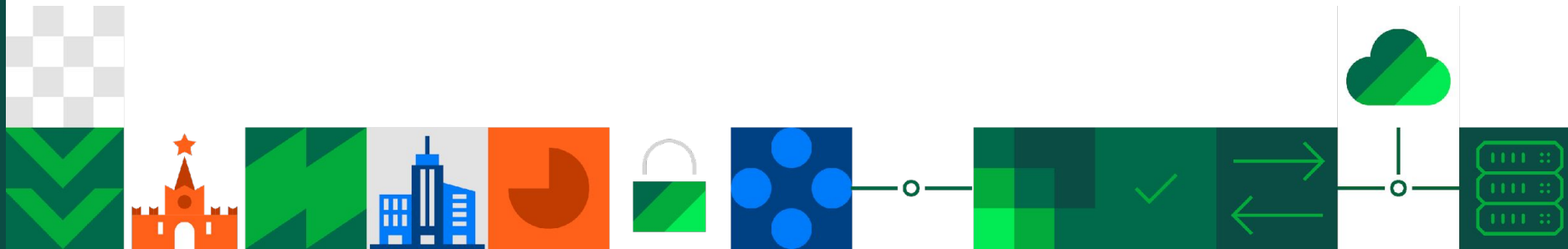
Security Gateway - node-1111

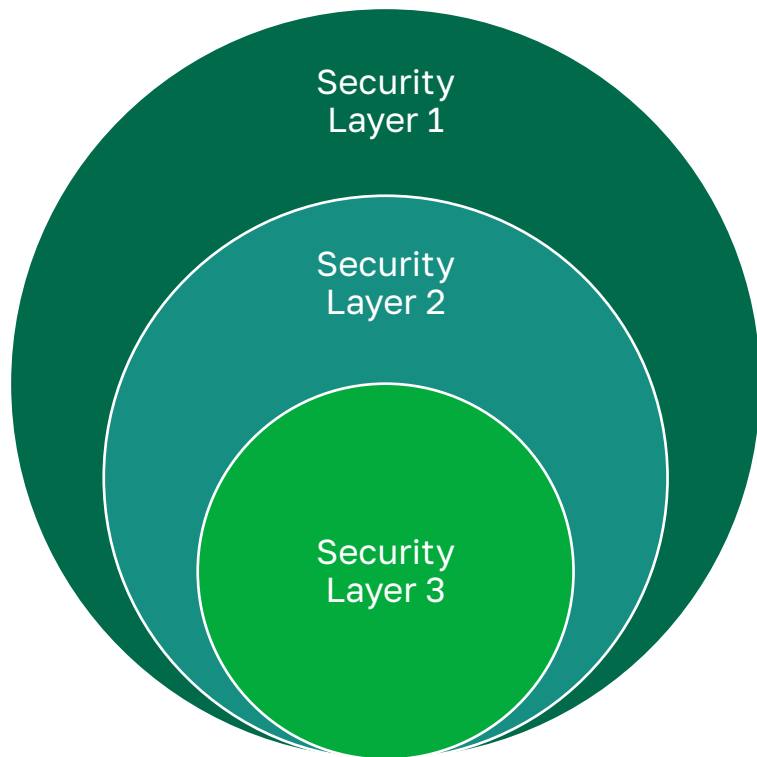
Components

- ☒ Security Management Server
- ☒ Firewall
 - ☐ Advanced Protocol and Application Control
 - ☒ Malicious URL Blocking
 - ☐ SkyDNS URL Blocking
 - ☒ Antivirus
 - ☐ Geo Protection
- ☐ QoS
- ☐ L2VPN
- ☒ L3VPN
- ☐ IPS
- ☐ Access Server
- ☐ User Identification
- ☐ Network Behavior Anomaly Detector (NBAD)



Components





Layer 1:

- Geo Protection
- Applications control (more 4000 apps)
- URL-filtering and categorize
- SSL-inspection (MiTM)

Layer 2:

- IDPS
- Threat Intelligence (IoC)
- Behavioral Analysis
- Antivirus

Layer 3:

- ICAP



Defining applications in network traffic

- Basic engine – 1700 apps
- Advanced engine – 4000 apps

URL-filtering

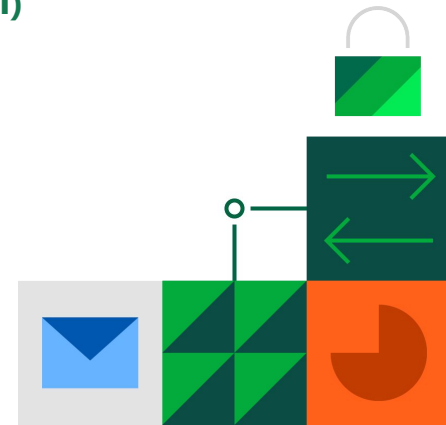
- Own black and white lists
- Predefined categories of sites

URL filtering via TLS/SSL-inspection

URL filtering via Server Name Indication (SNI)

Domain names in filtering rules (FQDN)

Filtering traffic based on countries (GeoIP)





Preventing network intrusions

- IPS signatures developed by our own laboratory
- The ability to work both on the network and on the channel levels

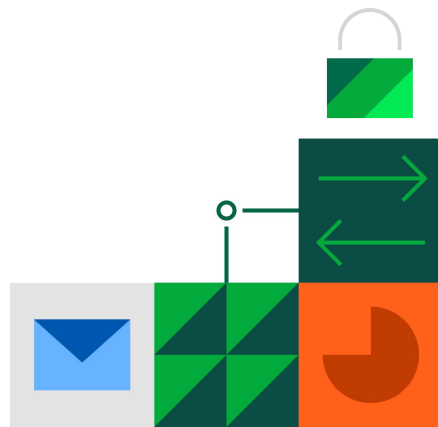
Threat Intelligence (IoC)

- Security Code
- Kaspersky Lab
- FinCERT (Russian Federation)
- RST-cloud

Analysis of network traffic for anomalies

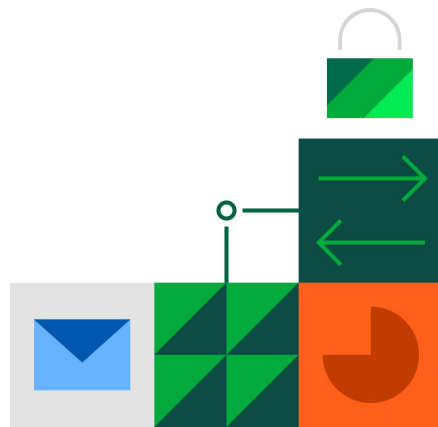
Antivirus traffic check

- Streaming Antivirus



Advanced malware search:

- Integration with Sandboxes via ICAP



Managing filtering rules

No.	Name	Source	Destination	Service	Protocol/Application	Action	Profile	IPS	Time	Log	Install On
SSH-connect											
1	To SN	192.168.1.0/24-SMS-net	ssh.mycompany.com	SSH	* Any	Accept	* None	Off	* Always	Log	* All
DMZ											
2	To DMZ	Россия	WEB-server-192.168.80....	HTTP ICMP TLS	* Any	Accept	* None	On	* Always	Log	NGFW
VPN-L3											
Internet											
4	DNS	192.168.1.0/24-SMS-net 192.168.20.0/24-SN-net-2 192.168.30.0/24-SN-net	* Any	DNS DNS	dns	Accept	* None	Off	* Always	None	* All
5	Application Control Access	192.168.20.0/24-SN-net-2	* Any	* Any	Social anydesk telegram telegram	Accept	* None	Off	* Always	None	NGFW
6	Application Control Deny	* Any	* Any	* Any	anydesk telegram telegram tor tor	Drop	* None	Off	* Always	None	NGFW
7	Web Access For Admins	admins@testlab.local a.popov	* Any	TLS	* Any	Filter	HTTPS-profile for Users	Off	* Always	Log	NGFW
DPI											
8	SN-inspection	192.168.20.0/24-SN-net-2	SSH-server-192.168.1.4	SSH	ssh	Accept	* None	Off	* Always	None	* All
9	WEB-Inspection	* Any	WEB-server-192.168.80....	HTTP TLS	http ssl	Accept	* None	Off	* Always	None	* All

Countries

IP addresses

Domain names

Enabling IPS

Gateway to which the policy is being set

Local or domain users

Filtering conditions

- URL Filtering Profile;
- TI feeds;
- AV/ICAP-check

Sections (6), Rules (15)

Search...

No.	Name	Source	Destination	Service	Protocol/Application	Action
Internet						
4	DNS	192.168.1.0/24-SMS-net 192.168.20.0/24-SN-net-2 192.168.30.0/24-SN-net	* Any	DNS DNS	dns	Accept
5	Application Control Access	192.168.20.0/24-SN-net-2	* Any	* Any	Social anydesk telegram telegram	Accept
6	Application Control Deny	* Any	* Any	* Any	anydesk telegram telegram tor tor	Drop
7	Web Access For Admins	admins@testlab.local a.popov	* Any	TLS	* Any	Filter
DPI						
8	SN-inspection	192.168.20.0/24-SN-net-2	SSH-server-192.168.1.4	SSH	ssh	Accept

Objects

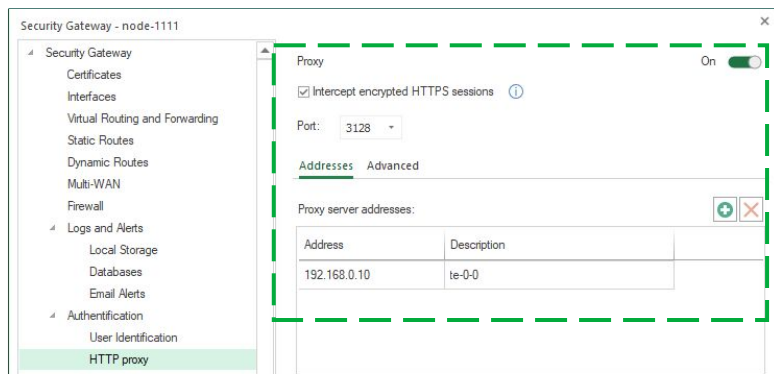
Tunnel

Name	Category	Type	Set	Parent	Description
Tunnel	-	-	-	-	-
actmobile-services	Tunnel	Application	Advanced		Actmobile Services
actmobile-services	Tunnel	Protocol	Advanced		Actmobile Services
act-vpn	Tunnel	Protocol	Advanced		Act VPN
act-vpn	Tunnel	Application	Advanced		Act VPN
amaze-vpn	Tunnel	Application	Advanced		Amaze VPN
anchorfree-services	Tunnel	Protocol	Advanced		Anchorfree Services

Groups, application protocols, categories, applications

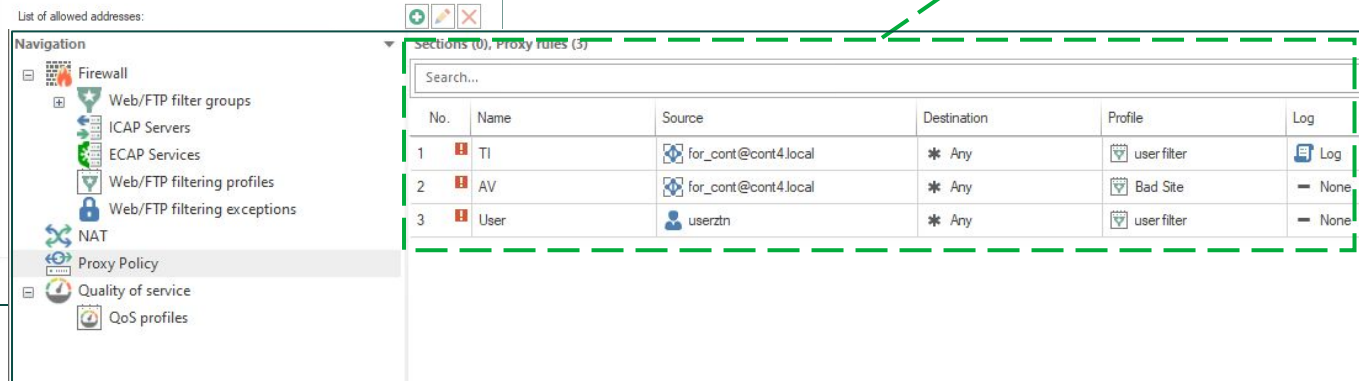
Search

List of applications



System settings for Proxy Server

Proxy Server policies





Navigation

IPS Policy

IPS Profiles

Security Code IPS Protections

Custom IPS Protections

Custom signatures

IPS protections (30 891)

Search...

IPS protection							IPS profile				
Severity	Description	Industry reference	Release date	Last update	Class	SID	IPS-profile	Оптимальный н...	Полный набор	Рекомендован...	
High	Successful Australian Government my...	None	14.12.2022	14.12.2022	Phishing	4142893	Drop	Inactive	Alert	Inactive	
High	Nemucod Downloading Payload 2	None	16.10.2015	04.06.2020	Trojan	4121957	Drop	Alert	Alert	Alert	
High	PowerTrick download ver2 bot	None	14.01.2020	14.01.2020	Trojan	4129274	Drop	Alert	Alert	Alert	
High	Filenam server.exe Download - Comm...	None	16.01.2015	14.05.2020	Trojan	4120202	Drop	Alert	Alert	Alert	
High	DustySky Downeks/Quasar/other DN...	None	31.01.2017	17.09.2020	Trojan	4123807	Drop	Alert	Alert	Alert	
High	W32/Bapy.Downloader PE Download ...	None	05.09.2014	25.09.2020	Trojan	4119128	Drop	Alert	Alert	Alert	
High	Possible Covenant Framework Grunt S...	None	04.08.2019	04.08.2019	Trojan	4127796	Drop	Alert	Alert	Alert	
High	Pony Downloader HTTP Library MSIE ...	None	13.04.2012	05.11.2020	Trojan	4114563	Drop	Alert	Alert	Alert	
High	Likely Geodo/Emotet Downloading PE	None	05.03.2014	18.04.2022	Trojan	4118225	Drop	Alert	Alert	Alert	
High	Kimsuky CSPY Downloader Activity	None	03.11.2020	03.11.2020	Trojan	4131172	Drop	Alert	Alert	Alert	
High	Pingback Download Command Issued	None	05.05.2021	10.05.2021	Trojan	4132918	Drop	Alert	Alert	Alert	
High	Possible ReactorBot .bin Download	None	27.05.2016	30.10.2020	Trojan	4122842	Drop	Pass	Alert	Alert	
High	WS/JIS Downloader Mar 07 2017 M1	None	08.03.2017	18.08.2020	Trojan	4124036	Drop	Inactive	Alert	Alert	

Info

Kimsuky CSPY Downloader Activity

Details

SID:

Severity:

Industry references:

Release date:

Last update:

Class:

4131172

High

None

03.11.2020

03.11.2020

Trojan

Hyperlinks

<https://www.cybereason.com/blog/back-to-the-future-inside-the-kimsuky-kgh-spyware-suite>

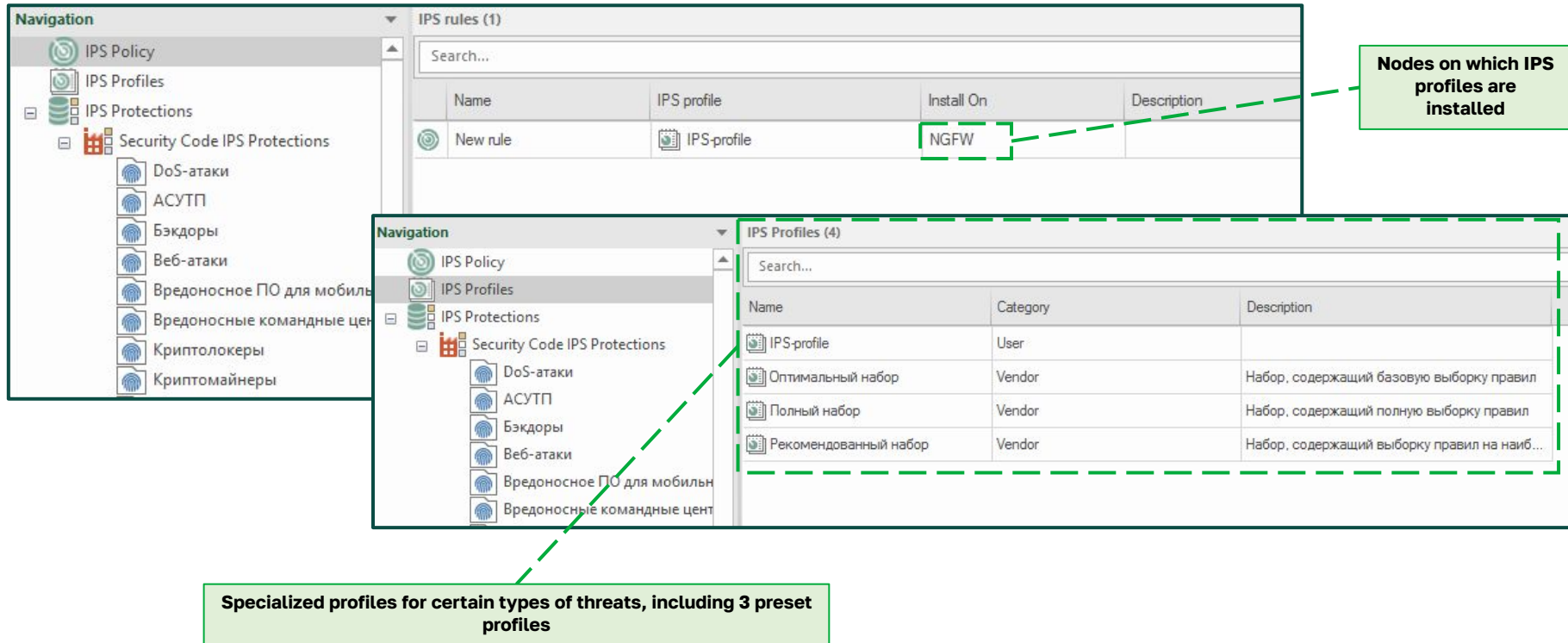
Access control

VPN

IPS

Structure

Administration



The screenshot displays the IPS Management interface, divided into two main sections. The top section, titled "IPS rules (1)", shows a table with columns: Name, IPS profile, Install On, and Description. A new rule is listed with the name "New rule", the profile "IPS-profile", and the installation point "NGFW". A green dashed box highlights the "NGFW" value, with a callout box stating: "Nodes on which IPS profiles are installed".

The bottom section, titled "IPS Profiles (4)", shows a table with columns: Name, Category, and Description. It lists four profiles: "IPS-profile" (User), "Оптимальный набор" (Vendor), "Полный набор" (Vendor), and "Рекомендованный набор" (Vendor). A green dashed box highlights the "Оптимальный набор", "Полный набор", and "Рекомендованный набор" profiles, with a callout box stating: "Specialized profiles for certain types of threats, including 3 preset profiles".

The left sidebar contains a "Navigation" menu with the following items:

- IPS Policy
- IPS Profiles
- IPS Protections
 - Security Code IPS Protections
 - DoS-атаки
 - АСУТП
 - Бэкдоры
 - Веб-атаки
 - Вредоносное ПО для мобильных устройств
 - Вредоносные командные центры
 - Криптолокеры
 - Криптомайнеры

Security Gateway - NGFW

User Identification

Interfaces

Static Routes

Dynamic Routes

Multi-WAN

Firewall

Logs and Alerts

Local Storage

Databases

Email Alerts

DNS

DHCP

SNMP

Hosts

SNMP Trap

SSH

LLDP

NetFlow

Collectors

Date and Time

NBAD

Attack Types

Mode: Learning by time ⓘ

Learning duration: 48 hours

Action: Alert

Blocking time: 300 seconds

☐ Reset statistics after policy installation

List of known network attack types:

State	Name	Exception
<input type="checkbox"/>	DNS Max Length	— No
<input type="checkbox"/>	Packet Sanity	— No
<input type="checkbox"/>	UDP Scan	— No
<input type="checkbox"/>	DNS Reply Mismatch	— No
<input type="checkbox"/>	LAND Attack	— No
<input type="checkbox"/>	FIN/RST Flood	— No

A machine learning
system is used



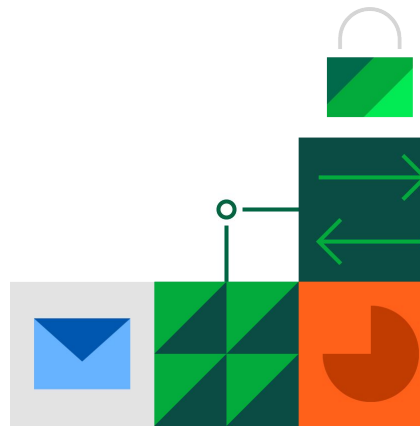
Virtual Routing (VRF)

Dynamic Routing

- OSPF
- BGP

Support for:


- Traffic Prioritization (QoS)
- Multi-WAN Connections
- VLAN Technology (IEEE802.1Q)
- Jumbo Frames
- LLDP
- BFD




Security Gateway - node-1111

- Security Gateway
 - Certificates
 - Interfaces
 - Virtual Routing and Forwarding
 - Static Routes
 - Dynamic Routes
 - Multi-WAN
 - Firewall
- Logs and Alerts
 - Local Storage
 - Databases
 - Email Alerts
- Authentication
 - HTTP proxy

Connection persistence

☐ Local 

☒ Global 

VRF zones

VRF zones list:

Name	Table	Description
vrf-001	1001	
vrf-002	1002	

Assignment of Interfaces in VRF


VRF

Overview Static Routes

ID: 1

Description:

Interfaces

Specify interfaces for virtual routing: 

Name	Type	Address/Mask
te-1-0	Ethernet	
te-1-0.2	VLAN	2.2.2.2/24

VRF Tables

Sections (0), QoS rules (1)

Search...

No.	Name	Filter					Action	
		Source	Destination	Service	Traffic Classifier	Transferred, MB	Remark	Priority
1		LAN	user1	* Any	Critical Data Network Control Scavenger Voice	* All	BE	Highest

QoS policies

Traffic classes

Objects

Search...

Name	Description
Best Effort	Undifferentiated applications
Call Signalling	SCCP, SIP, H.323
Critical Data	ERP Apps, CRM Apps, Dat...
Interactive Video	Video presentation
Network Control	OAM&P, EIGRP, OSPF, BG...
Scavenger	YouTube, iTunes, BitTorrent...

QoS Profile

Name: Out

Description:

Traffic type: Outbound traffic

Bandwidth


☐ Limited by interface bandwidth
☒ Upload bandwidth 100 Mbps

Queues


Priority	Reserved bandwidth, %		Bandwidth, Mbps
	Minimum	Maximum	
Medium High	0	100	0 - 100
Medium	0	100	0 - 100
Medium Low	0	100	0 - 100
Lowest	100	100	100


QoS profiles setup




Multi-WAN





On 


☒ Reset sessions at connections change





☒ Automatic hide NAT 












WAN connections: 

Name	Interface	Default gateway	Detection	Description
wan1	 te-1-0	1.1.1.50	 On	wan1
wan2	 te-1-...	3.3.3.5	 On	

WAN rules: 

No.	Source	Destination	Service	Interface	Type	Connections
1	 user1	* Any	* Any	# Auto	Exclude	— None
2	 192.168.0.0...	* Any	 LDAPS-TCP  LDAPS-UDP  NTP-UDP  POP3-UDP	# Auto	Failover	 wan1 (1)  wan2 (2)
3	 LAN	* Any	* Any	# Auto	Balancing	 wan2 (1)  wan1 (1)

Multi-WAN rules



L3 VPN and L2 VPN

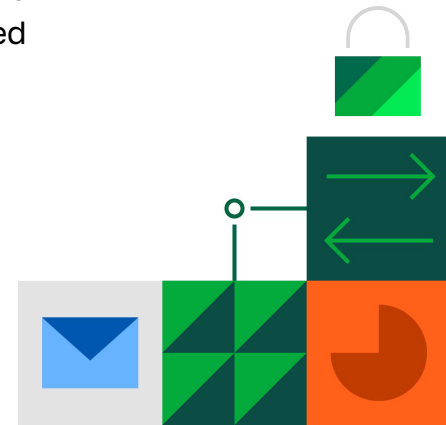
Topologies:

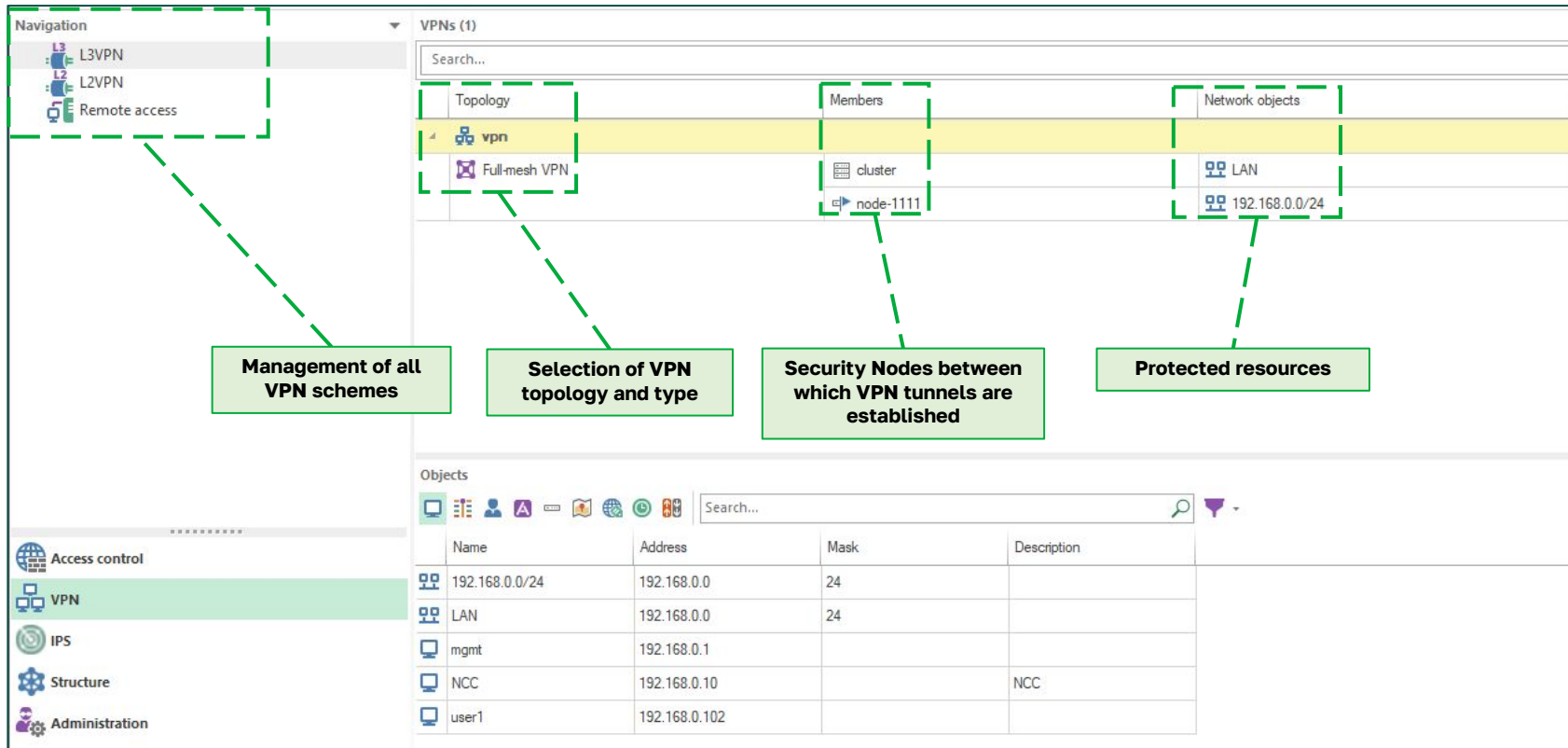
- Full Mesh Network
- Star

VPN Traffic Firewall Policy:

- Interfaces directed to the Internet
- Interfaces directed to internal (local) networks
- Schedule limiting VPN operation time
- Types of data that can be transmitted

NAT translation within VPN





The screenshot displays the VPN Management interface. The left sidebar contains a 'Navigation' menu with 'L3VPN', 'L2VPN', and 'Remote access'. The main area shows 'VPN (1)' with a search bar and three tabs: 'Topology', 'Members', and 'Network objects'. The 'Topology' tab is active, showing a 'vpn' object and a 'Full-mesh VPN' option. The 'Members' tab shows a 'cluster' and 'node-1111'. The 'Network objects' tab shows 'LAN' and '192.168.0.0/24'. Below the tabs is an 'Objects' table with columns for Name, Address, Mask, and Description. The table lists several objects including '192.168.0.0/24', 'LAN', 'mgmt', 'NCC', and 'user1'. The bottom sidebar contains a menu with 'Access control', 'VPN', 'IPS', 'Structure', and 'Administration'. Four green dashed boxes with arrows point from descriptive text boxes to specific interface elements: 'Management of all VPN schemes' points to the Navigation menu; 'Selection of VPN topology and type' points to the 'Full-mesh VPN' option; 'Security Nodes between which VPN tunnels are established' points to 'node-1111'; and 'Protected resources' points to the 'Network objects' tab.

Management of all VPN schemes

Selection of VPN topology and type

Security Nodes between which VPN tunnels are established

Protected resources

Name	Address	Mask	Description
192.168.0.0/24	192.168.0.0	24	
LAN	192.168.0.0	24	
mgmt	192.168.0.1		
NCC	192.168.0.10		NCC
user1	192.168.0.102		

Navigation

- L3VPN
- L2VPN
- Remote access

Remote access rules (3)

Search...

No.	Name	Users	Authentication method	Access	Connection control	Allow edit access servers list	Multiple con...	Time	Install On
1		userztn	Certificate or passw...	LAN	No control	Allow	Allow	* Always	cluster
2		for_cont@cont41...	Password	LAN	Deny unsecured con...	Allow	Allow	* Always	cluster
3		userztn	Password		Redirect through tun...	Disabled	Allow	* Always	All

Remote access policies

User list

Objects

Search...

Name	Address	Mask	Description
192.168.0.0/24	192.168.0.0	24	
LAN	192.168.0.0	24	
mgmt	192.168.0.1		
NCC	192.168.0.10		NCC
user1	192.168.0.102		

Access control

VPN

IPS

Structure

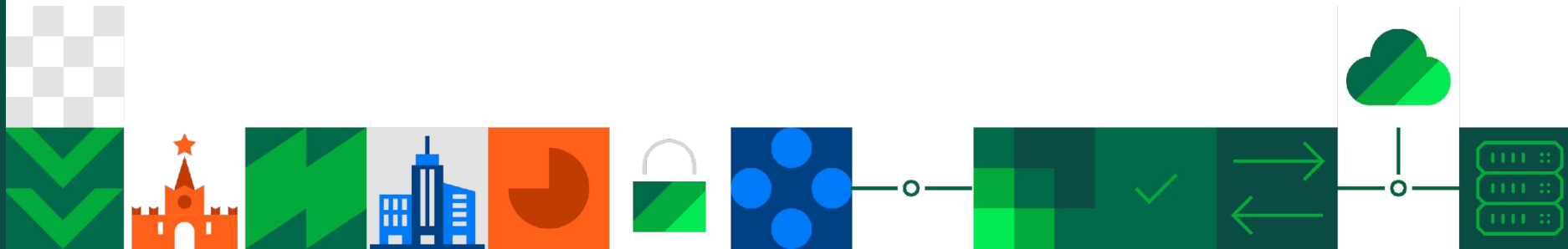
Administration

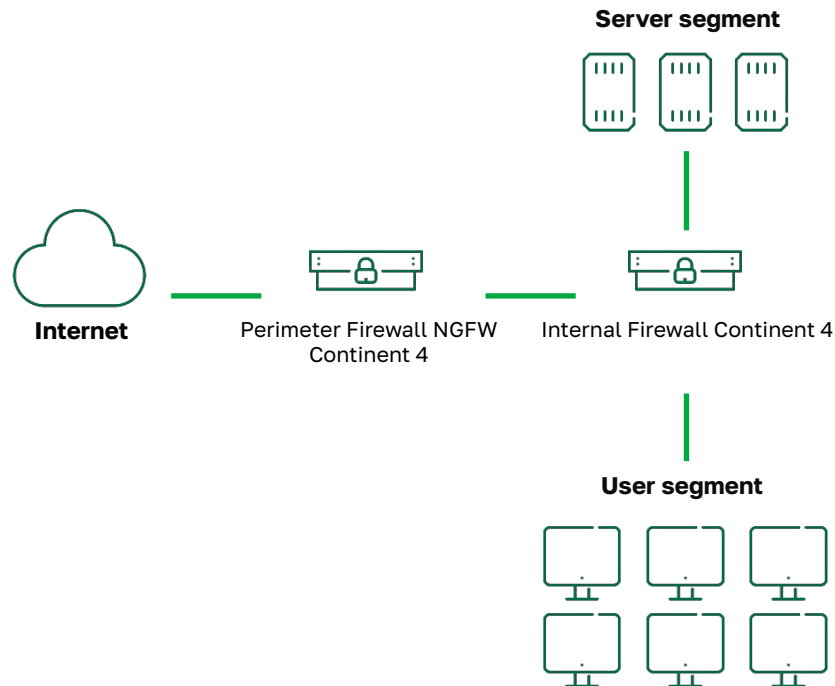


SECURITY
code



Operating modes





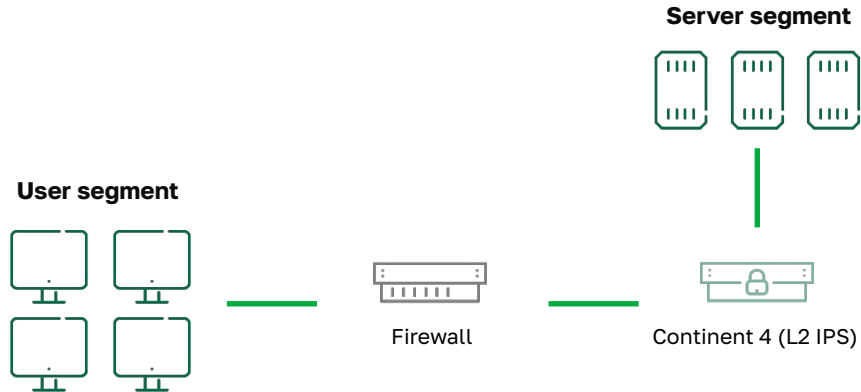
Tasks

- Protection of interactions with the Internet
 - User identification
 - Intrusion detection/prevention
 - Application control
 - URL filtering
 - Connection of remote users
 - Creation of secure communication channels
- Isolation of network segments
 - High throughput for any packets
 - Ability to work with extensive traffic filtering policies
 - High level of fault tolerance



Tasks

- Detection of network threats



Junior performance



- IPC-R10
- IPC-R50
- IPC-10
- IPC-50

Medium performance



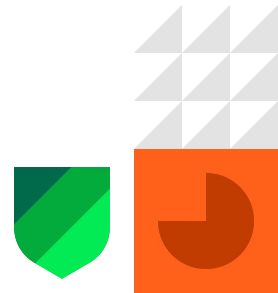
- IPC-R300
- IPC-R550
- IPC-R800
- IPC-3000F LE

High performance



- IPC-R1000
- IPC-R1000 NF2
- IPC-R3000
- IPC-3000F
- IPC-3000F40
- IPC-3000NF2

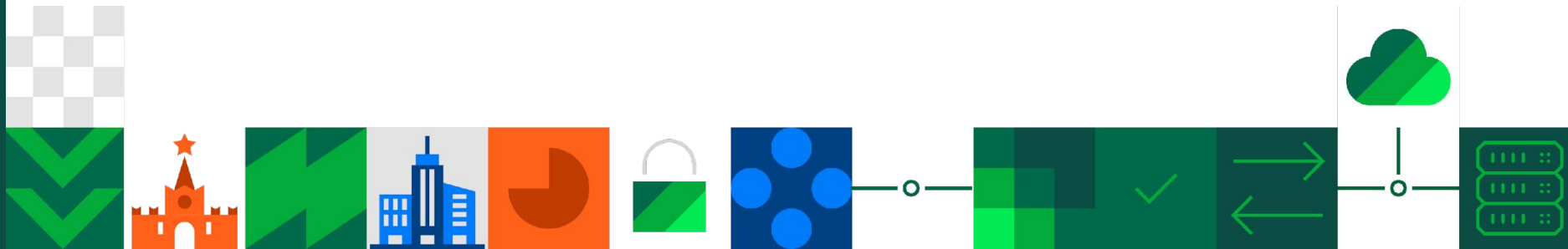
Name	Number of cores	FW, Mbit/s	UTM, Mbit/s	L2 IPS, Mbit/s
SOHO	2	4 000	700	1 000
SMB	4	12 000	2 500	2 000
ENT	8	16 000	6 000	5 500



Модуль	Security Node	Basic UTM	Advanced UTM
Network Control Center	✓	✓	✓
Firewall	✓	✓	✓
Access Server	✓	✓	✓
Application control (1700 protocols and apps)	✓	✓	✓
URL filtering	✓	✓	✓
Advanced application control (4000 protocols and apps)		✓	✓
Intrusion detection system		✓	✓
GeoIP traffic blocking		✓	✓
Malicious site protection			✓
Pre-configured URL categories			✓
Stream antivirus			✓
High-performance firewall (NF2)	Not included in the Security Node (SN)/UTM, purchased separately. License duration is perpetual.		
L2 VPN	Not included in the Security Node (SN)/UTM, purchased separately. License duration is perpetual.		



10. *Journal of the American Academy of Religion*, 47 (1979), 1–22.



Single security architecture

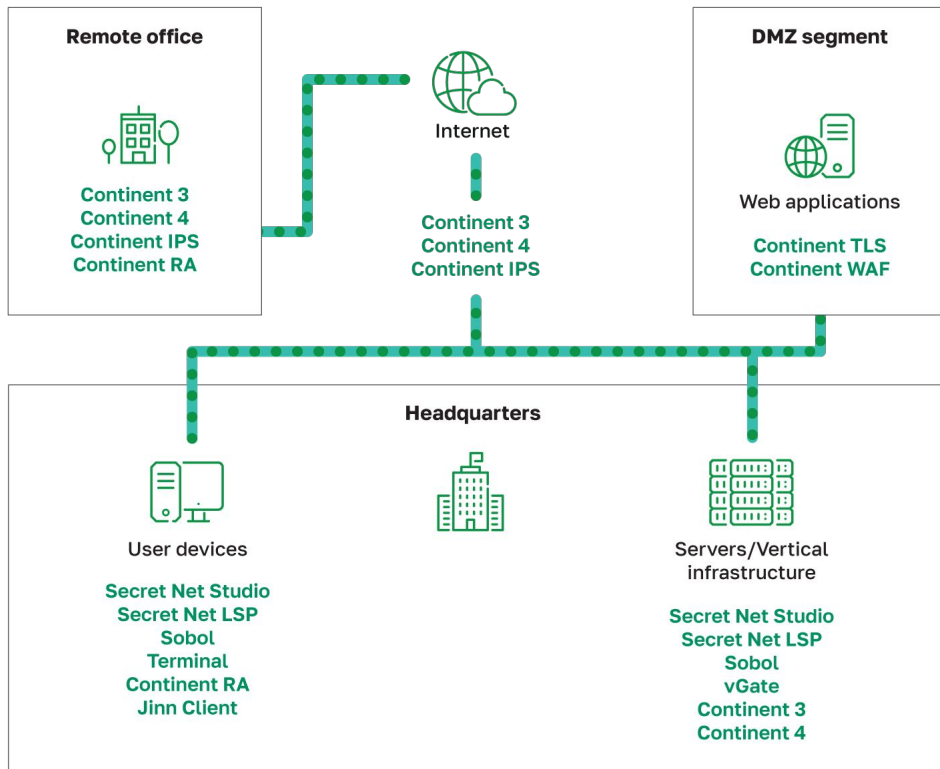
Security Code develops a few product lines following the same architectural concept aimed at providing security for different information system components. This approach makes it possible for our customers to develop their information security systems step-by-step by adding new elements that will extend functionality of earlier deployed security tools.

Centralized management and monitoring

All Security Code products provide centralized management of security policies, security tool state monitoring and prompt alert notification. On top of that, integration with SIEM systems is also provided.

Guaranteed product compatibility

All Security Code products are compatible with each other and ensure correct operation and interaction of different elements of an information security system. When using several Security Code products, customers can make use of additional security management mechanisms simplifying the configuration and use of the products.



Company «Security code» – is a Russian developer of software and hardware solutions that ensure the protection of information systems and their compliance with international and industry standards.

- **For over 30 years**, Security Code has been safeguarding the security of the largest enterprises in Russia.
- It operates under 9 licenses from **FSTEC**, **FSB**, and **the Ministry of Defense of Russia**.
- Its protection technologies ensure the security of **3 000 000** computers across **50 000** organizations.
- **The company has 3 development centers:** Moscow, St. Petersburg, and Penza.
- There are more than **800 qualified R&D specialists** with unique competencies.
- **Over 50** security solutions and cryptographic security tools have been developed.
- More than **60 active certificates** of compliance confirm the high quality of its products.
- The company's partner network includes **over 1 000 authorized partners**.

The competence of Security Code is confirmed by independent analysts:

- «Largest manufacturers of high-tech equipment»: №1 («Expert RA»), №3 («Kommersant»).
- «Largest software developers»: №7 («Expert RA»), №9 («Kommersant»).
- «Largest IT companies in Russia»: №30 («Kommersant»), №47 (TAdviser).

Government Organizations:



Федеральное казначейство России



Федеральная налоговая служба России



Федеральная таможенная служба России



Федеральный Фонд обязательного медицинского страхования



Центральная избирательная комиссия Российской Федерации



Министерство юстиции Российской Федерации

Law Enforcement Agencies:



Министерство внутренних дел Российской Федерации



Министерство обороны Российской Федерации



Федеральная служба безопасности Российской Федерации



Федеральная служба охраны Российской Федерации

Telecommunications Companies:



ПАО «Ростелеком»



ПАО «МГТС»



ГК «АКАДО Телеком»



АО «Воентелеком»

Financial Institutions:



ПАО «Сбербанк»



Центральный банк Российской Федерации



ГК «Внешэкономбанк»



АО «Газпромбанк»



ПАО «Промсвязьбанк»



Банк ВТБ (ПАО)



ПАО «Московский кредитный банк»



АО «АЛЬФА-БАНК»

Industrial Enterprises:



ГК «Ростех»



АО «Российские космические системы»



НОРНИКЕЛЬ

ПАО «ГМК «Норильский никель»



ГК «Росатом»



ПАО «Газпром»



Транснефть

ПАО «АК «Транснефть»



ROSNEFT

ПАО «НК «Роснефть»»

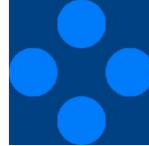


ПАО «Россети»

Energy Sector Enterprises:



Documentation on Continent 4



Thank you!

Headquarters: Moscow, 1st Nagatinskij proezd, 10, bldg. 1

Service center: Moscow, Elektrolitnyj proezd, 9, bldg. 1

Phone: +7 (495) 982-30-20

E-mail: info@securitycode.ru

www.securitycode.ru
