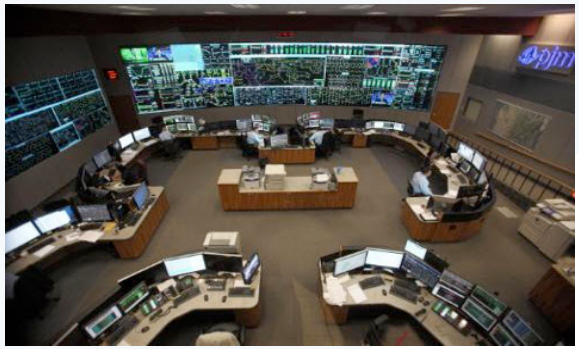
Сети АСУТП: мифы и реалии



Евгений Кутумин

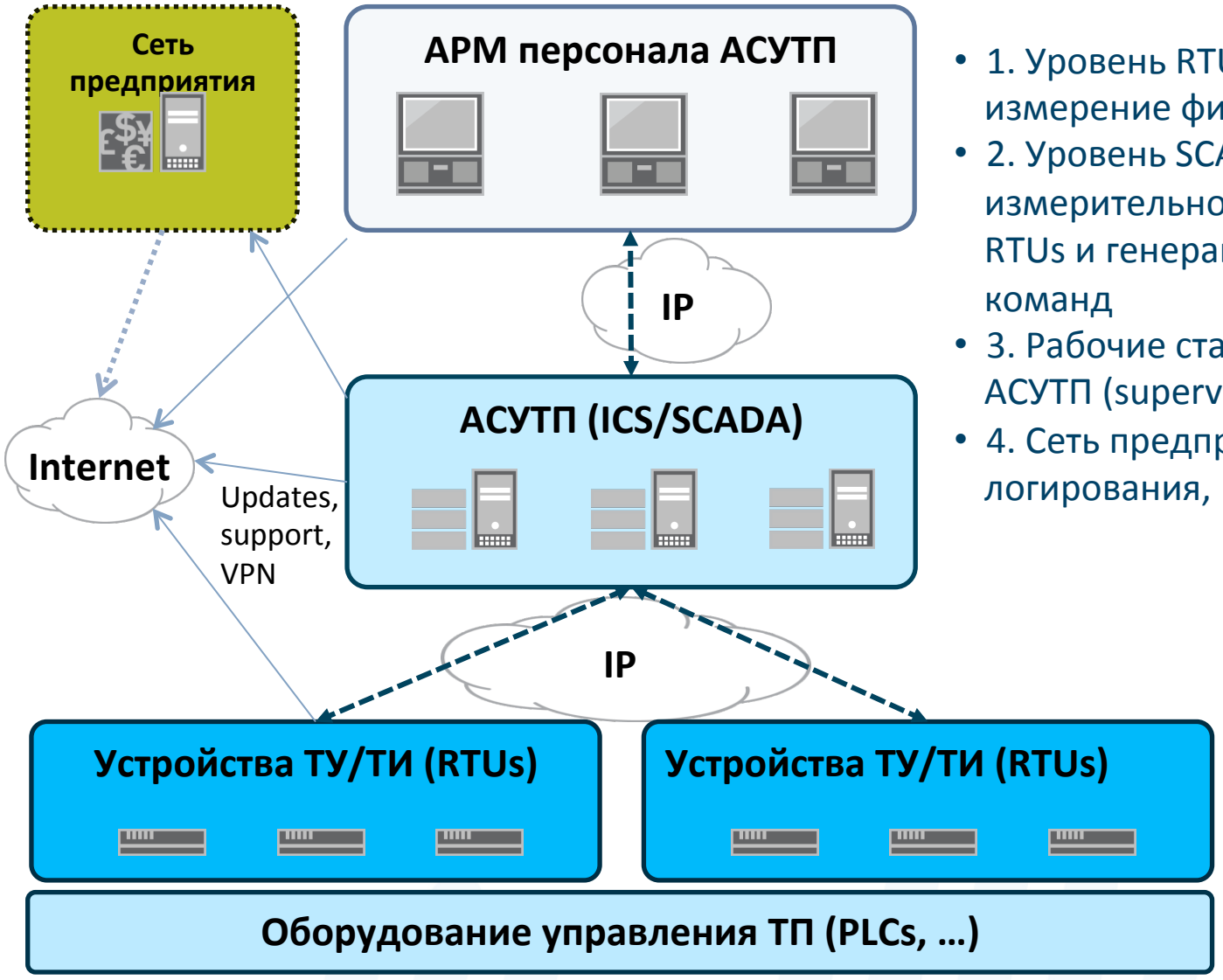
системный инженер

Palo Alto Networks

paloalto NETWORKS

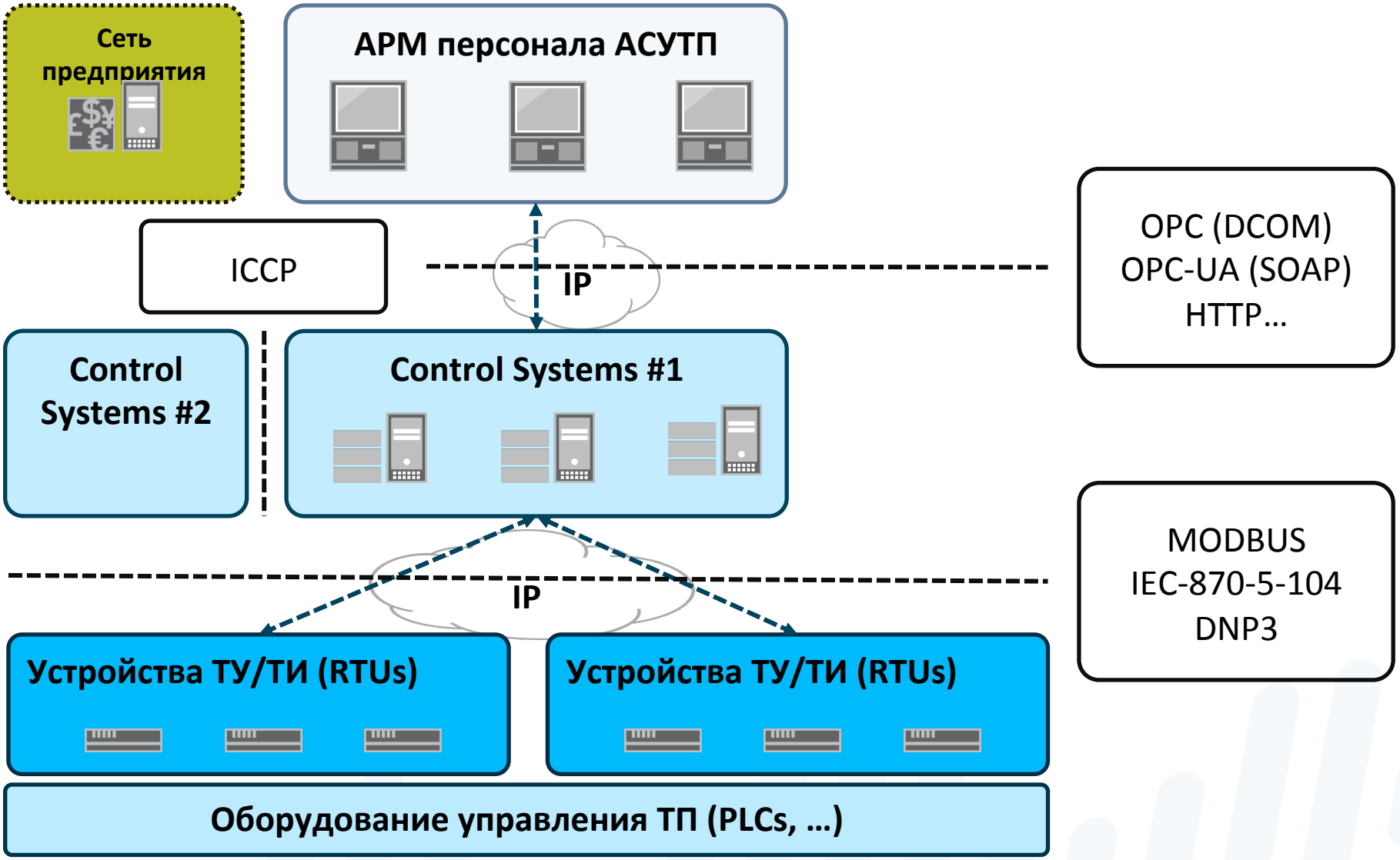
the network security company™

Типовая обобщенная схема сети производственного предприятия



- 1. Уровень RTUs & PLCs: контроль и измерение физических сигналов
- 2. Уровень SCADA: агрегирование измерительной информации от RTUs и генерация управляющих команд
- 3. Рабочие станции персонала АСУТП (supervisors)
- 4. Сеть предприятия: системы логирования, ERP и проч.

Протоколы, используемые в сетях АСУТП



paloalto NETWORKS

Нужно ли защищать сети АСУТП?

Историческая картина:

- АСУТП-системы и проприетарные протоколы управления неизвестны и неинтересны хакерам;
- Сеть АСУТП изолирована от корпоративной сети и сети Интернет, что делает сетевые атаки в реальном времени невозможными
- Нет вирусов

Современная реальность:

- Используются протоколы согласно индустриальным стандартам, мигрированные в IP;
- Многие SCADA, RTUs используют протоколы общего назначения HTTP, FTP, TFTP,…;
- Интеграция с ERP и др. бизнес системами для учета продукции;
- Используется удаленный доступ через Интернет для обслуживания производителем;
- Используются Интернет-каналы для доступа к удаленным объектам (VPN);
- Используются съемные накопители (USB flash), способствующие инфицированию

paloalto NETWORKS

Нужно ли защищать сети АСУТП?

Особенности ПО АСУТП:

- Несегментированные («плоские») сети;
- Протоколы изначально разработаны для выделенных физических каналов связи => нет шифрования и аутентификации;
- Проблематично обновление и установка патчей для ОС и прикладного ПО критических систем управления реального времени (неизменные версии сроком 5/10/15 лет) => уязвимости;
- ПО разрабатывалось для решения прикладных задач без оглядки на безопасность => уязвимости, пароли по умолчанию, нет разделения прав пользователей (общие учетные записи)

Итог:

- Риск DoS (финансовый и/или физический ущерб)
- Риск кражи технологической информации
- Популярность атак на АСУТП пром. предприятий и комм. ЦОД

Примеры вирусов в сетях АСУТП

Stuxnet (Иран, 2010г.): 3 уровня атаки (в т.ч. «нулевого дня»)

- MS Windows: копирование с USB, распространение по RPC, P2P;
- SCADA-система Siemens (PCS 7, WinCC, STEP7): модификация библиотеки, перехват коммуникаций между SCADA и PLC;
- Siemens S7 PLCs: инсталляция в память PLC вредоносного ПО, которое меняет частоту подключенного электромотора.

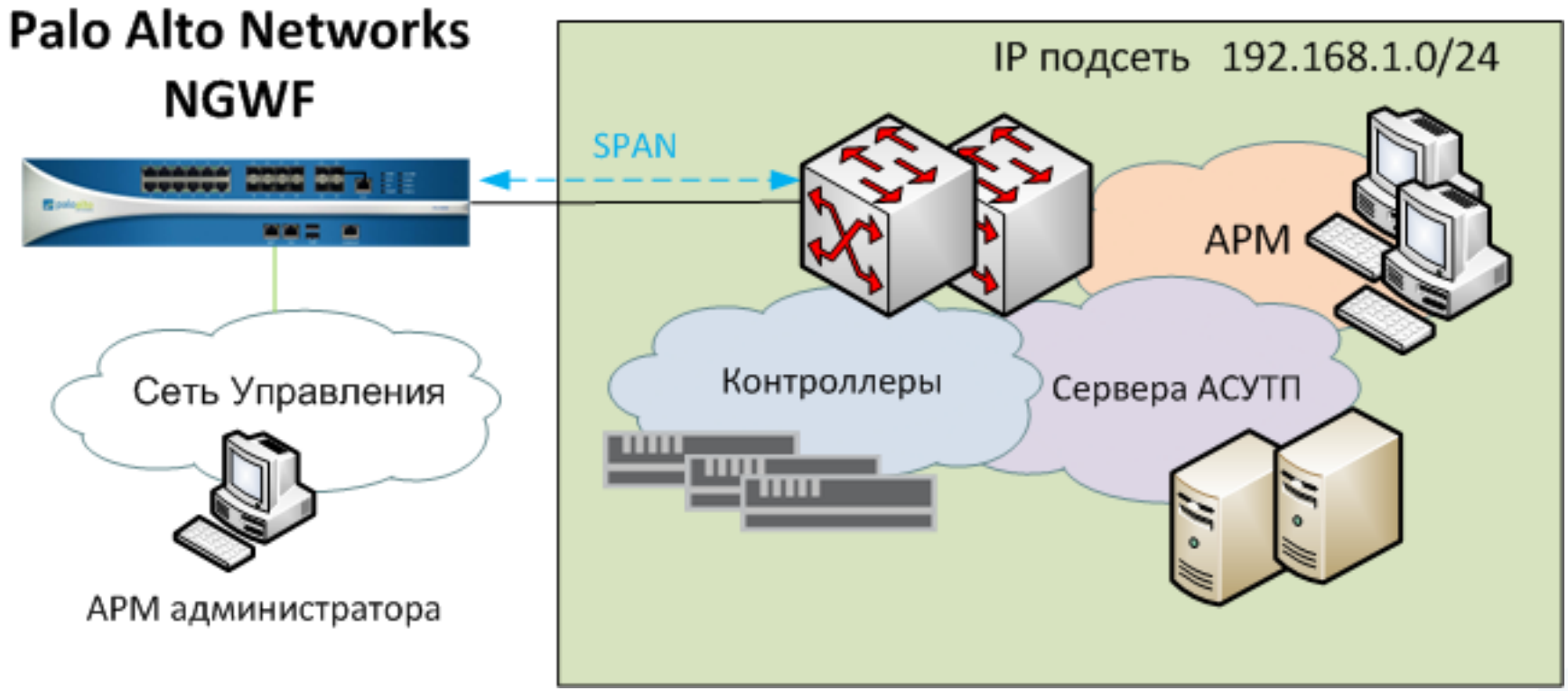
Duqu (2011г.):

- В отличие от Stuxnet пытается организовать удаленный доступ с целью получения технологической информации

FLAME (2012 г.):

- В 20 раз сложнее Stuxnet, код вируса был написан за 5 лет до первой атаки;
- Распространение по всему ближнему востоку, включая Иран, Израиль/ Палестин, Судан, Сирию, Ливан, Саудовскую Аравию, Египт. Вирус также был замечен в Венгрии, Австрии, Гонконге и в **РОССИИ.**

Пример выявленных угроз в изолированной сети АСУТП одного из Заказчиков в РФ



Пример выявления угроз в изолированной сети АСУТП

Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
2	ldap	business-systems	auth-service	client-server	105,768,162	47,177
2	kerberos	business-systems	auth-service	client-server	60,995,860	48,149
2	active-directory	business-systems	auth-service	client-server	42,239,314	9,020
2	ms-netlogon	business-systems	auth-service	client-server	20,104,300	15,076
2	postgres	business-systems	database	client-server	3,660,250,616	50,748
3	ms-sms	business-systems	management	client-server	569,353,821	5,292
1	eset-update	business-systems	software-update	client-server	69,422,058	8,063
4	ms-update	business-systems	software-update	client-server	44,128,328	3,505
3	ms-ds-smb	business-systems	storage-backup	client-server	1,183,293,896,942	159,865
2	wuala	general-internet	file-sharing	client-server	584,351,444	21
5	ftp	general-internet	file-sharing	client-server	44,248,296	1,482
5	emule	general-internet	file-sharing	peer-to-peer	5,106,772	3,055
5	webdav	general-internet	file-sharing	browser-based	228,993	24
2	ping	general-internet	internet-utility	network-protocol	113,505,712	745,487
4	web-browsing	general-internet	internet-utility	browser-based	9,760	4
2	rtp	media	photo-video	client-server	102,323,800	18
2	netbios-ss	networking	infrastructure	network-protocol	62,383,345,041	23,189
4	dns	networking	infrastructure	network-protocol	112,407,525	472,821
2	msrpc	networking	infrastructure	network-protocol	38,432,131	37,770
2	netbios-ns	networking	infrastructure	network-protocol	10,760,548	8,424
2	netbios-dg	networking	infrastructure	network-protocol	5,875,061	23,171
1	upnp	networking	infrastructure	peer-to-peer	624,822	128
1	ssdp	networking	infrastructure	peer-to-peer	279,907	56
2	ntp	networking	infrastructure	network-protocol	169,622	1,491
2	llmnr	networking	infrastructure	network-protocol	82,732	609
2	dhcpv6	networking	infrastructure	network-protocol	28,658	62
2	dhcp	networking	infrastructure	network-protocol	20,998	53
4	icmp	networking	ip-protocol	network-protocol	18,542,812	108,207
1	ipv6-icmp	networking	ip-protocol	network-protocol	7,090	8
2	telnet	networking	remote-access	client-server	298,027	35
1	igmp	networking	routing	network-protocol	9,736,926	99

Пример выявления угроз в изолированной сети АСУТП

Отчет по приложениям с высоким риском (4-5):

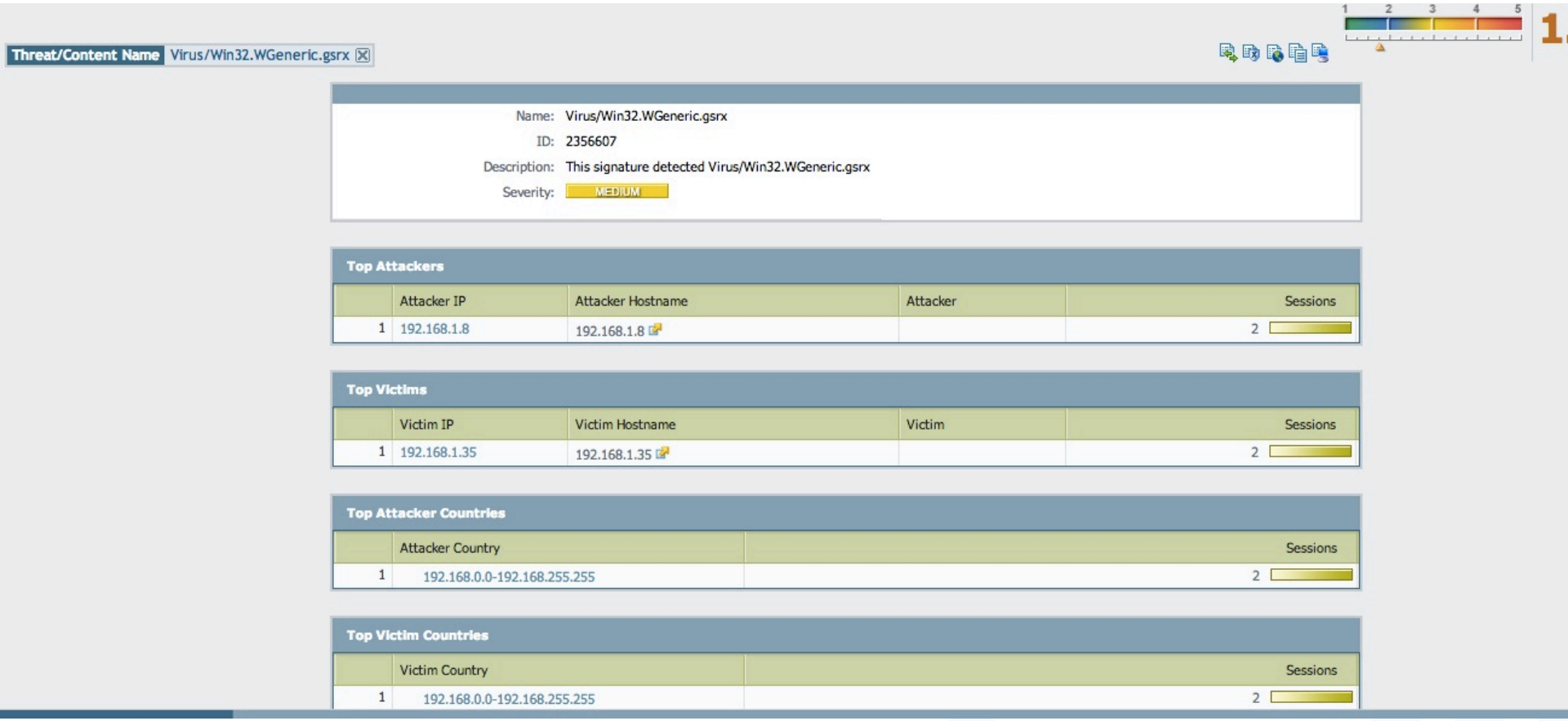
Risk	Application	Category	Sub-Category	Technology	Bytes	Sessions
4	ms-update	business-systems	software-update	client-server	44,128,328	3,505
5	ftp	general-internet	file-sharing	client-server	44,248,296	1,482
5	emule	general-internet	file-sharing	peer-to-peer	5,106,772	3,055
5	webdav	general-internet	file-sharing	browser-based	228,993	24
4	web-browsing	general-internet	internet-utility	browser-based	9,760	4
4	dns	networking	infrastructure	network-protocol	112,407,525	472,821
4	icmp	networking	ip-protocol	network-protocol	18,542,812	108,207

Отчет по пользователю:

Risk	Application	App Category	App Sub Category	App Technology	Sessions	Bytes
2	vnc-encrypted	networking	remote-access	client-server	2	47.8M
1	unknown-udp	unknown	unknown	unknown	2.1k	10.0M
1	insufficient-data	unknown	unknown	unknown	2.8k	4.4M
5	ftp	general-internet	file-sharing	client-server	31	3.8M
4	dns	networking	infrastructure	network-protocol	3.9k	1.3M
2	telnet	networking	remote-access	client-server	25	272.4k
2	netbios-ns	networking	infrastructure	network-protocol	499	259.1k
2	rtp	media	photo-video	client-server	3	121.7k
2	llmnr	networking	infrastructure	network-protocol	982	116.6k
2	netbios-dg	networking	infrastructure	network-protocol	82	28.4k
1	ssdp	networking	infrastructure	peer-to-peer	4	4.8k
1	igmp	networking	routing	network-protocol	16	3.3k
2	dhcp	networking	infrastructure	network-protocol	3	1.0k
1	non-syn-tcp	unknown	unknown	unknown	4	730

paloalto NETWORKS

В изолированной сети АСУТП были обнаружены вирусы



Threat/Content Name: Virus/Win32.WGeneric.gsrx

Name: Virus/Win32.WGeneric.gsrx
ID: 2356607
Description: This signature detected Virus/Win32.WGeneric.gsrx
Severity: MEDIUM

Top Attackers

	Attacker IP	Attacker Hostname	Attacker	Sessions
1	192.168.1.8	192.168.1.8		2

Top Victims

	Victim IP	Victim Hostname	Victim	Sessions
1	192.168.1.35	192.168.1.35		2

Top Attacker Countries

	Attacker Country	Sessions
1	192.168.0.0-192.168.255.255	2

Top Victim Countries

	Victim Country	Sessions
1	192.168.0.0-192.168.255.255	2

Пример выявления уязвимостей в изолированной сети АСУТП

Threat Name	Application	Category	Severity	Count
Microsoft Windows Print Spooler Service Format String Vulnerability	netbios-dg	code-execution	Critical	2
Microsoft Windows SMB NTLM Authentication Lack of Entropy Vulnerability	ms-ds-smb		Medium	18
Netbios Small Piece Data Evasion Attack Vulnerability	ms-ds-smb	code-execution	Medium	8
SMB Fragment Packet Found	ms-ds-smb	info-leak	Medium	6
Microsoft DCE RPC Big Endian Evasion Vulnerability	msrpc	info-leak	Medium	4
SMB Data Segmented Across TCP Evasion Attack	ms-ds-smb	code-execution	Medium	1
Microsoft Windows Registry Read Attempt	msrpc	info-leak	Low	74
Microsoft Windows WinReg Access Attempt	ms-ds-smb	code-execution	Low	66
Microsoft Windows Date and Time Enumeration	msrpc	info-leak	Low	32
Microsoft ASP.Net Information Leak Vulnerability	ms-sms	info-leak	Low	2
Microsoft ASP.Net Information Leak Vulnerability	ms-sms	brute-force	Low	2
Microsoft ASP.Net Information Leak Vulnerability	ms-update	info-leak	Low	1
Microsoft ASP.Net Information Leak Vulnerability	ms-update	brute-force	Low	1
Microsoft Windows SMB Negotiate Request	ms-ds-smb		Informational	109
Microsoft RPC Endpoint Mapper	msrpc	info-leak	Informational	49
Microsoft Windows Server Service NetrServerGetInfo access	msrpc	info-leak	Informational	35
Microsoft Windows user enumeration	msrpc	info-leak	Informational	24
Microsoft Windows Server Service NetrShareEnum access	msrpc	info-leak	Informational	24
Windows Local Security Architect LsarQueryInformationPolicy	msrpc	info-leak	Informational	18
Microsoft Windows Registry Enumeration	msrpc	info-leak	Informational	13
NetBIOS nbtstat query	netbios-ns	info-leak	Informational	11
Service Enum Through SMB ServiceEnum2	ms-ds-smb	info-leak	Informational	9
Windows SMB Login Attempt	ms-ds-smb	brute-force	Informational	2
HTTP OPTIONS Method	webdav	info-leak	Informational	1

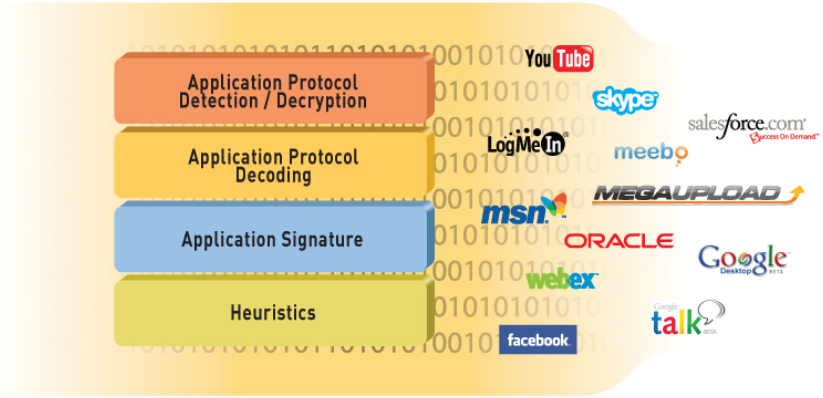
Чем могут помочь межсетевые экраны нового поколения Palo Alto Networks для защиты IP-сетей АСУТП ????

paloalto NETWORKS

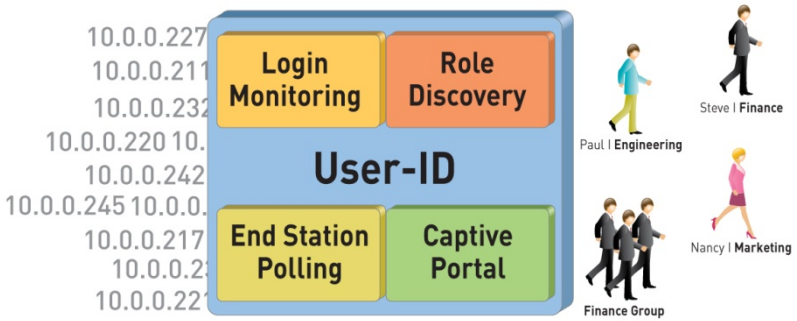
Технологии NGFW Palo Alto Networks

FIREWALL

App-ID™
Идентификация приложений



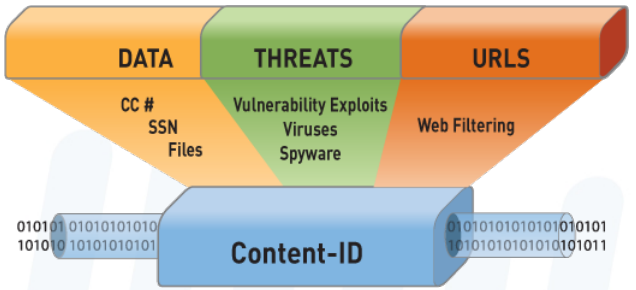
User-ID™
Идентификация пользователей



THREAT PREVENTION

Content-ID™
Контроль данных

+ SSL decryption



paloalto NETWORKS

Контроль приложений SCADA на L7 (App-ID)

- **«Положительная» логика применения политик безопасности** – неизвестные приложения эффективно блокируются по умолчанию
- **Специализированные протоколы SCADA:**
  - MODBUS с 15 контролируемыми функциями (read/write);
  - DNP3;
  - IEC-870-5-104;
  - ICCP;
  - CygNet, BACnet;
- **Протоколы общего назначения:**
  - HTTP, HTTPS, FTP, TFTP, OPC, RPC…
- **Анализ SPAN и широкие возможности создания собственных сигнатур приложений**
- **Дешифрация SSL**

paloalto NETWORKS

Контроль действий пользователей (User-ID)

Реализация функций идентификации пользователей (операторов и администраторов АСУТП):

- интеграция с сетевыми каталогами (при наличии):
  - Microsoft, Novell, Citrix, Open LDAP, RADIUS;
- возможность использования встроенного Captive Portal:
  - локальная база пользователей, LDAP, RADIUS;
- возможность интеграции с внешним веб-сервером аутентификации и Security Operations Center (SOC) через XML API.

Контроль действий (только чтение, отправка управляющих воздействий и др.) – политики безопасности разрешают отдельным пользователям и группам использовать только определенные подприложения (функции), для которых созданы отдельные сигнатуры.

paloalto NETWORKS

Защита от угроз (Content-ID)

70+ сигнатур IPS для протоколов Modbus, DNP3, ICCP и SCADA систем:

- Siemens Tecnomatix FactoryLink;
- Siemens SIMATIC WinCC;
- Iconics Genesis (+GenBroker);
- Interactive Graphical SCADA system (IGSS);
- CitectSCADA;
- Measuresoft ScadaPro;
- DATAC RealWin;
- PROMOTIC;
- KingView;
- ScadaTec.

Контроль передачи файлов по типам (исполняемые и др.)

- **Антивирусная защита**:
  - StuxNet;
  - Duqu, Flame, MiniFlame и др.
- **Обнаружение нового вредоносного ПО (zero-day)**
  - Публичное или частное облако WildFire обеспечивают анализ 100+ типов поведения
  - Публичное облако создает сигнатуры AV в течение 30 (мин.)

paloalto NETWORKS

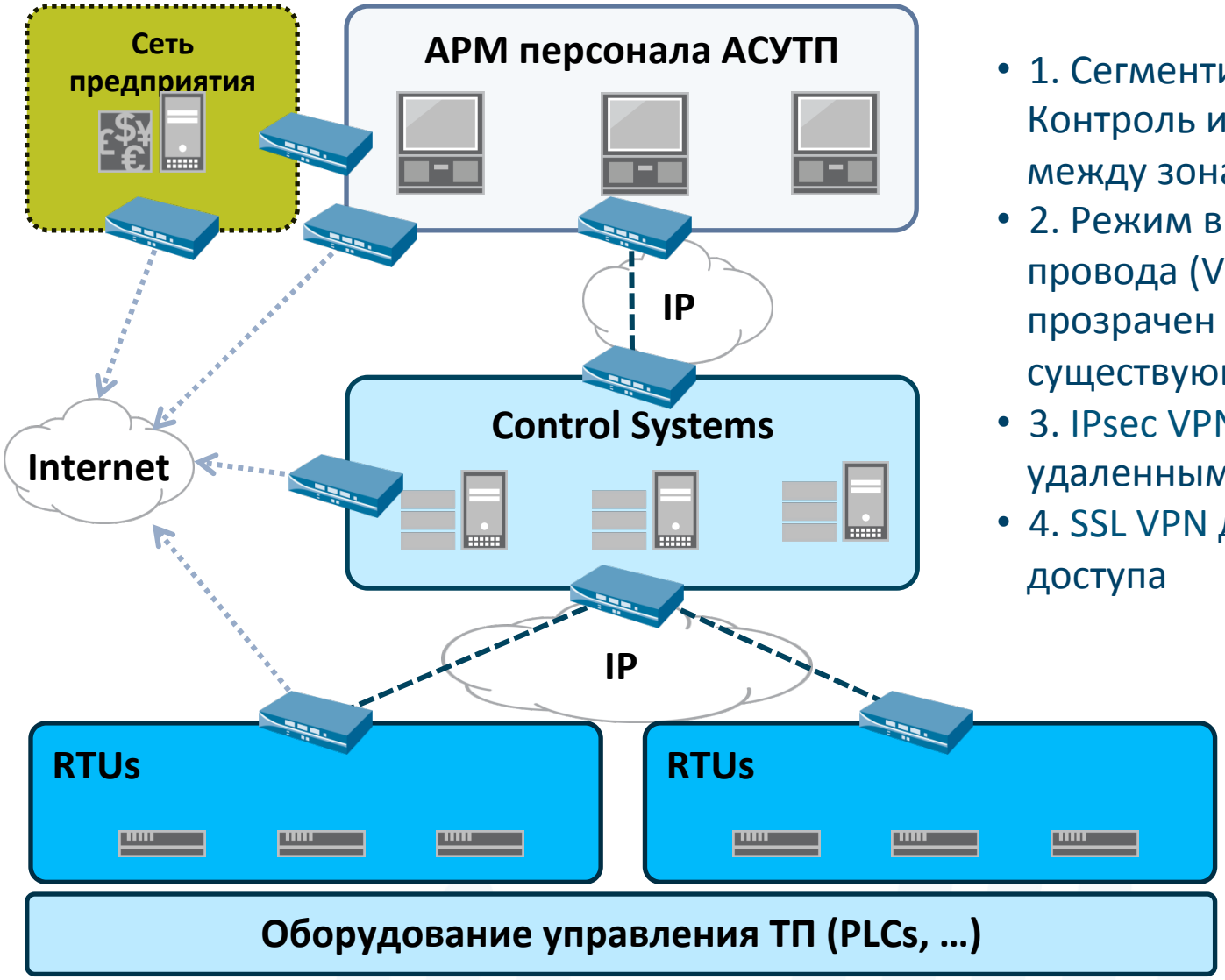
Как работает сервис WildFire

Автоматическая или по запросу
генерация сигнатуры в «облаке»

Изолированная сеть

- Анализируется 100+ типов поведения;
- WF-500 проверяет 4500 файлов в день: исполняемые, офисные, PDF, JAVA;
- Сигнатура автоматически создается и загружается на все устройства в течение 30 мин.
- 40% новых экземпляров – это вариации одних и тех же вредоносов;
- 1 сигнатура покрывает до 1500+ уникальных хэшей SHA

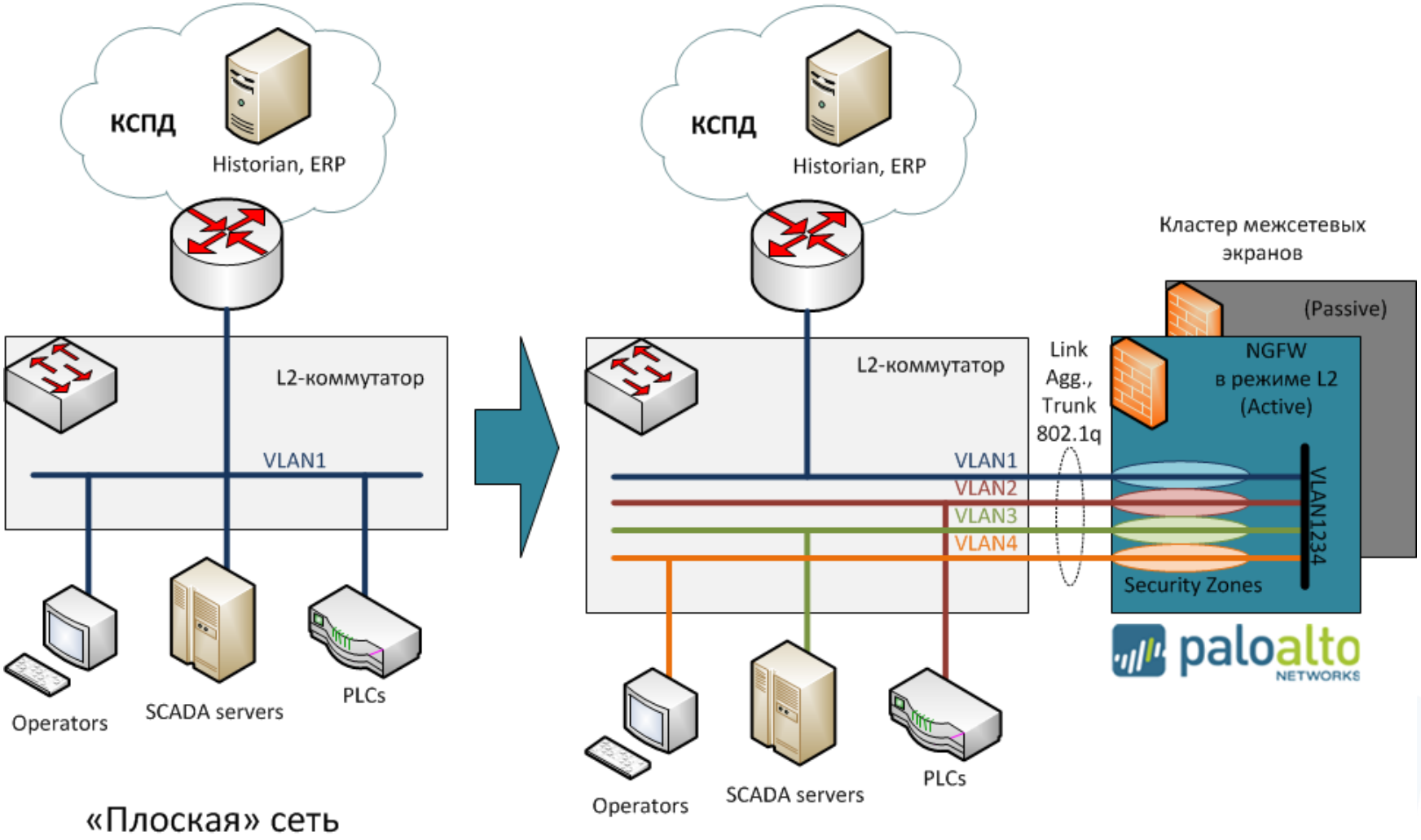
Создание зон безопасности с использованием межсетевых экранов нового поколения (сегментирование)



- 1. Сегментирование сети. Контроль и анализ трафика между зонами
- 2. Режим виртуального провода (Vwire), L2 – прозрачен для существующих SCADA систем
- 3. IPsec VPN для связи с удаленными объектами
- 4. SSL VPN для удаленного доступа

paloalto NETWORKS

Пример сегментирования сети АСУ ТП на уровне L2: «Firewall on a stick»



Примеры компаний, использующих Palo Alto Networks для защиты АСУТП:

Страна	Название/характеристика компании	Ссылки и примечания
Норвегия	Несколько энергетических компаний, в т.ч. гидроэнергетика	Крупные проекты, в т.ч. более $1M
США	Douglas County PUD (Public Utility District)	http://www.douglaspud.org/
США	United Illuminating	www.uinet.com
США	Tri State Generation	http://www.tristategt.org/
Канада	Enmax	http://www.enmax.com/home.html Контроль протоколов MODBUS, DNP3, ICCP
Австралия	Australian Power & Gas (APG)	https:// www.australianpowerandgas.com.au
Австралия	Australian Energy Market Operator (AEMO)	http://www.aemo.com.au/

paloalto NETWORKS