WATERFALL®
Stronger Than Firewalls

EnergySec
The National Energy Sector Cyber Security Organization

Maximize Security to Minimize Compliance Costs

Technical Solutions Focused Webinar
July 28, 2015
Sponsored by Waterfall Security Solutions

Agenda

- Welcome and Panel Introduction
- Goals
- Why consider unidirectional gateway
- Provide examples of real generating utilities using unidirectional gateway-based networks
- Use attack modeling to compare firewall and unidirectional gateway defensive capabilities
- Compare the cost of managing and monitoring strong unidirectional vs firewalled networks
- Questions

Meet Your Panelists

Andrew Ginter
VP, Industrial Security
Waterfall Security

Karl Perman
VP, Services
EnergySec

Steve Parker
President
EnergySec

It’s Interactive

Please submit your questions through the control panel to get answers LIVE from our panelists.

Webinar Goals

- Offer insights and potential approaches pertaining to unidirectional gateway-based networks.
- Provide examples of real generating utilities using a new, comprehensive model for unidirectional gateway-based networks.
- Apply the unidirectional gateway model to generating-unit segmentation advice.
- Use attack modeling to compare firewall and Unidirectional Gateway defensive capabilities.
- Compare the cost of managing and monitoring strong unidirectional vs firewalled networks.

Why Consider Unidirectional Gateway

- Provides level of security
- NERC CIP language calls out bi-directional routable protocols
  - Mitigate number of requirements
- Can be used to segment generating units and their associated BES Cyber Systems
- Combination of hardware and software
- Newer generation of security technology

WATERFALL®
Stronger Than Firewalls
CYBERSECURITY 500
WORLD'S HOTTEST SECURITY COMPANIES
FROST & SULLIVAN
2012 BEST PRACTICES AWARD
NORTH AMERICAN NETWORK SECURITY FOR INDUSTRIAL CONTROL SYSTEMS ENTREPRENEURIAL COMPANY OF THE YEAR AWARD
FROST & SULLIVAN
2013 BEST PRACTICES AWARD
NORTH AMERICAN DEFENSE-IN-DEPTH PLATFORM FOR UPSTREAM OIL & GAS CUSTOMER VALUE ENHANCEMENT AWARD
FROST & SULLIVAN
2014 BEST PRACTICES AWARD
GLOBAL OIL AND GAS INFRASTRUCTURE SECURITY NEW PRODUCT INNOVATION LEADERSHIP AWARD

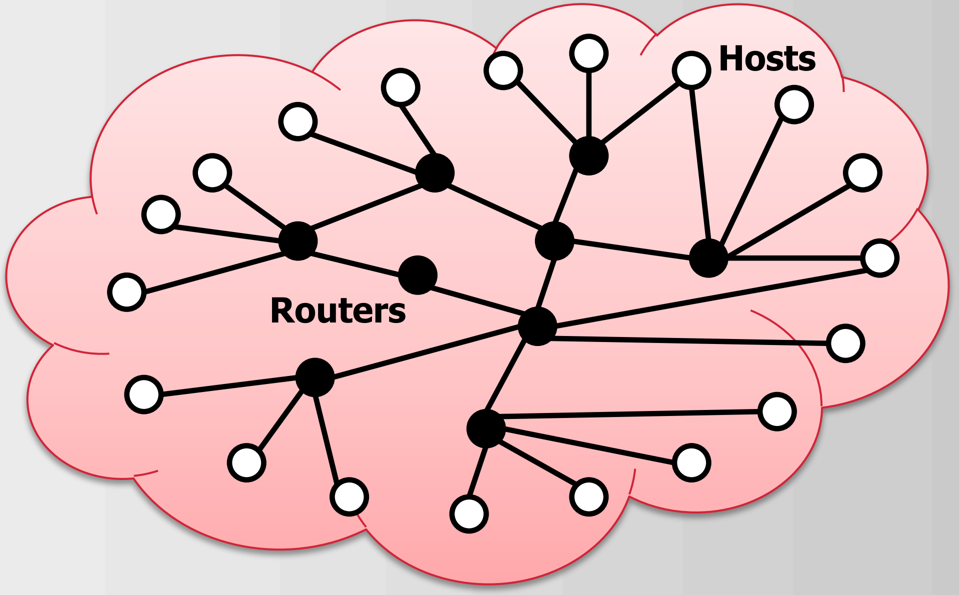
Maximize Security to Minimize Compliance Costs

Andrew Ginter, VP Industrial Security
Waterfall Security Solutions

Traditional Security: Firewalls Are Routers With Filters

- 99% of the Internet is hosts, routers and communications links:
  - Hosts are sources and destinations of messages
  - Routers forward messages through communications links
- Firewalls are routers with filters – the filter looks at each message and decides whether to forward it, or drop it
- No filter is or can ever be perfect

All firewalls forward attacks from external networks to "protected" networks



Traditional Security: Firewalls Are Porous

Attack Type	UGW	Fwall
1) Phishing / drive-by-download – victim pulls your attack through firewall	🟩	🟥
2) Social engineering – steal a password / keystroke logger / shoulder surf	🟩	🟫
3) Compromise domain controller – create ICS host or firewall account	🟩	🟥
4) Attack exposed servers – SQL injection / DOS / buffer-overflow	🟩	🟥
5) Attack exposed clients – compromised web svrs/ file svrs / buf-overflows	🟩	🟥
6) Session hijacking – MIM / steal HTTP cookies / command injection	🟩	🟥
7) Piggy-back on VPN – split tunneling / malware propagation	🟩	🟥
8) Firewall vulnerabilities – bugs / zero-days / default passwd/ design vulns	🟩	🟥
9) Errors and omissions – bad fwall rules/configs / IT reaches through fwalls	🟩	🟥
10) Forge an IP address – firewall rules are IP-based	🟩	🟥

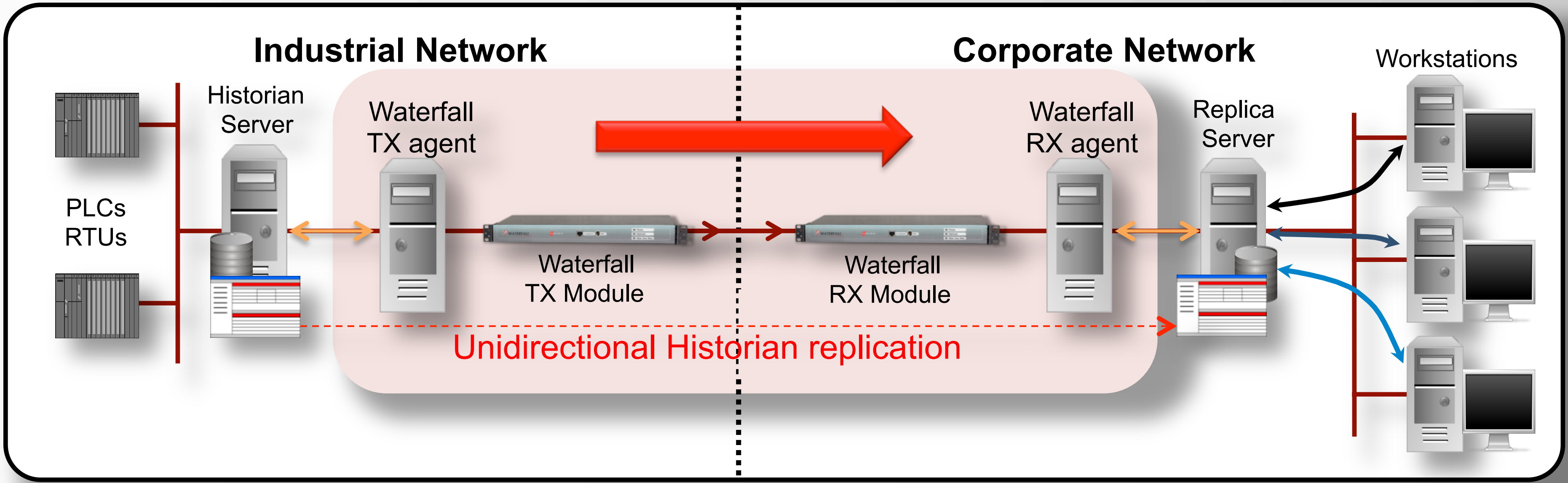
Attack Difficulty:	🟩 Impossible	🟥 Routine	🟫 Easy

Photo: Red Tiger Security

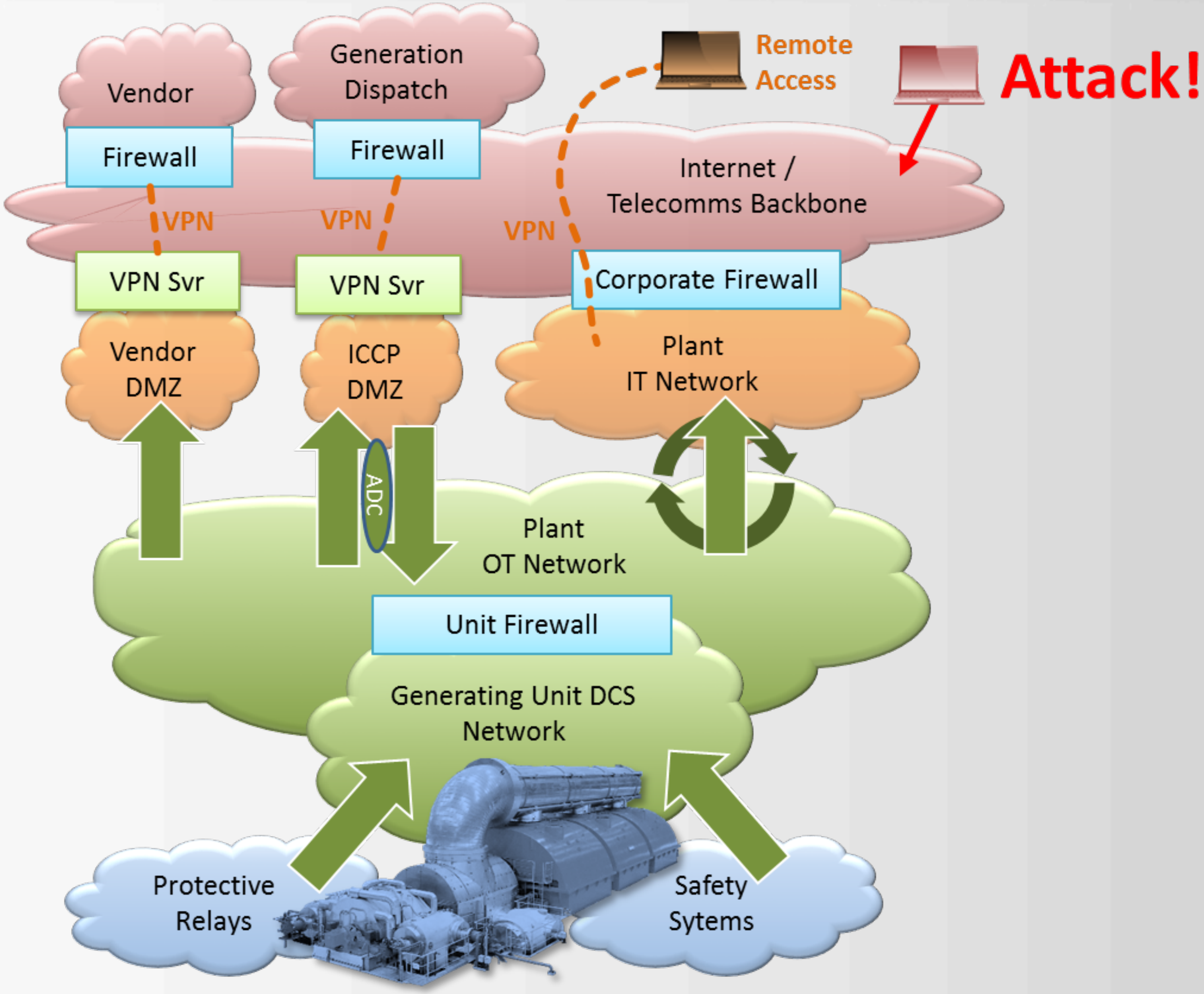
Firewall have been with us for 30 years now. The good guys and the bad guys both know how to defeat them.

Secure Unidirectional Server Replication

- Hardware-enforced unidirectional server replication
- Replica server contains all data and functionality of original
- Corporate workstations communicate only with replica server
- Industrial network and critical assets are physically inaccessible from corporate network & 100% secure from any online attack



Maximize Security with Modern Power Gen Networks



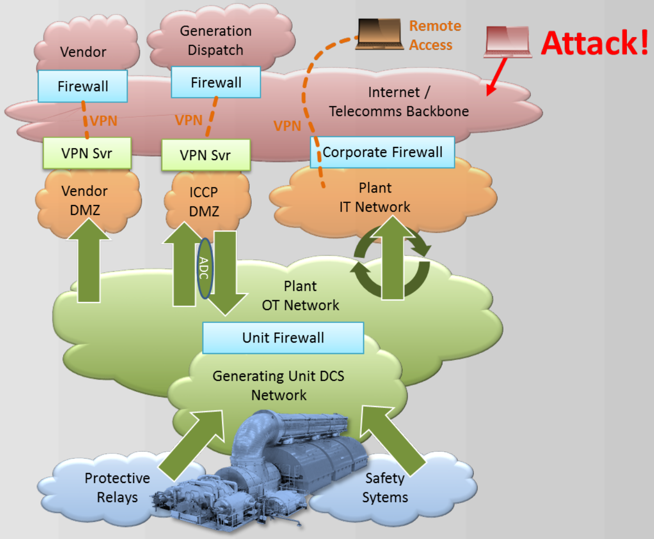
Strong Security Options for Network Integration

Product	Icon	Description
Unidirectional Security Gateway	→	Combination of hardware and software that replicates servers out of a control system only – physically impossible to send anything back into the protected network
Waterfall FLIP	🔄	A reversible Unidirectional Security Gateway. Replicates servers in one direction, or the other, but never both at the same time.
Inbound/Outbound Gateways	→ ▪▪▪▪▪▪▪▪▪ ←	One Unidirectional Security Gateway replicating servers in one direction. A second gateway independently replicates a different set of servers in the other direction.
Application Data Control	ADC	Software add-on providing fine-grain, policy-based inspection and control over industrial data flows, even for encrypted, compressed, proprietary and undocumented industrial protocols.
Secure Bypass	X SBP	For emergency access to networks during declared CIP emergencies.

Power Generation Use Cases For Maximum Reliability

- Safety systems – replicate Modbus servers and Syslog & SNMP clients
- Protection systems – replicate DNP3 & event log servers
- IT/OT integration – replicate historian & OPC servers and many others
  - Optional: FLIP to replicate security updates back in as well
- Generation dispatch – base load replicates ICCP server out
  - Peaking plant independently replicates ICCP server in as well
- Turbine vendor – replicate historian & other servers out to turbine vendor.
  - Remote Screen View for adjustments

At least one layer of unidirectional products breaks chain of attack from Internet through to ICS & protective relays



Maximum Security Minimizes NERC CIP V5 Costs

- CIP V5 encourages the use of Unidirectional Security Gateways
- External Routable Connectivity: *The ability to access a BES Cyber System that is accessible from a Cyber Asset that is outside of its associated Electronic Security Perimeter via a* ***bi-directional*** *routable protocol connection.*
- 38 of 129 medium-impact requirements apply only if the affected cyber asset has external routable connectivity

"When you are considering security for your control networks, you need to keep in mind innovative security technologies such as unidirectional gateways" *Tim Roxey, NERC CSSO*

NERC CIP V5 Compliance Savings Of Strong Security

CIP Standard	Total Requirements	ERC-Exempt Med Impact Requirements	ERC-Exempt High Impact Requirements
002 BES Cyber System Categorization	7	-	-
003 Security Management Controls	4	-	-
004 Personnel and Training	19	15	-
005 Electronic Security Perimeters	8	7	5
006 Physical Security of BES Cyber Systems	14	11	-
007 Systems Security Management	20	5	-
008 Incident Reporting & Resp. Planning	9	-	-
009 Recovery Plans	10	-	-
010 Change Mgmt & Vuln Assessments	10	-	-
011 Information Protection	4	-	-
014 Physical Security	24	-	-
Totals:	129	38	5

Proposed NERC CIP V6 preserves all of the above, and the new Low Impact External Routable Connectivity (LERC) definition also includes the word "bi-directional"

CIP Auditors Agree With Compliance Savings

- Q: Is External Routable Connectivity (ERC) possible through Unidirectional Security Gateways?
  - No.
  - No, though auditors would typically seek evidence that validates a unidirectional claim.
  - A Unidirectional Gateway configured to allow outbound traffic from the ESP but not allow inbound traffic to enter the ESP would effectively eliminate External Routable Connectivity.
- Q: Is Remote Screen View (RSV) Interactive Remote Access (IRC)?
  - No.
  - [With RSV] … the user-initiated process to push screen snapshots through the ESP is originating from within the ESP. By definition, that does not constitute Interactive Remote Access.

Traditional Generating Unit Segmentation

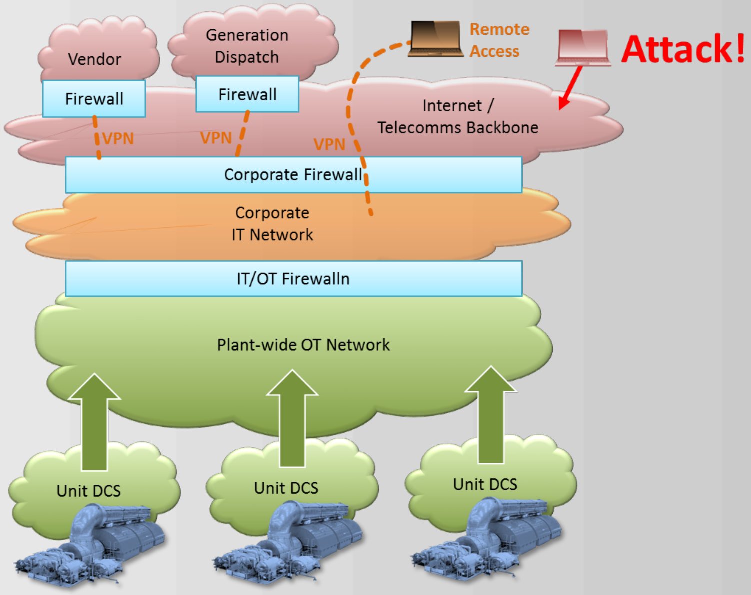
Entities may choose to segment generating units at a 1500 MW generation resource and their associated BES Cyber Systems such that each segmented unit, or group of units, and their associated BES Cyber Systems do not meet the 1500 MW criteria described in CIP-002-5.1, Attachment 1, Criterion 2.1. Segmenting generating units and their associated BES Cyber Systems can reduce risks to the reliable operation of the BES.

- Eliminate / duplicate shared systems, eg: coal feeds, air compressors
- Provide evidence of analysis, that no systems remain able to impact 1500MW or more within 15 minutes
- Demonstrate access restrictions on network interfaces *"(eg: firewall rules)"*

But: firewalls provide only minimal protection to segmented networks. How does this reduce risks to reliable operation of the BES?

Strong Security For Segmented Units Reduces Costs

- Take a tiny fraction of segmentation's CIP compliance cost savings and apply them to securing segmented DCS networks unidirectionally
- Strong security:
  - Breaks one large target into many smaller targets
  - Each smaller target is safe from simultaneous / coordinated attack from the Internet or corporate network
  - Dramatically reduce risk / cost of security incidents



Unidirectionally protecting segmented units is good business

Understanding Security With Attack Modelling

- Quantitative Risk (earthquakes, pandemic) = Likelihood * Cost
- Qualitative Risk (Cyber) = Threat * Vulnerability * Likelihood * Cost
  - Qualitative scores mean nothing to senior decision-makers
- Attack modelling – describe attacks, not qualitative risks
- Attack training / expertise is essential to defense
- Design basis threat: what is the simplest attack able to breach our defences with a high degree of confidence

No defense is perfect. Attack expertise is essential to evaluating a defensive posture

Minimum Compliance = Race For The Bottom

Disable safeties	Disable safeties	Local misoperation	Disable safeties	Disable safeties	Compromised insider
Rem targeted misoperation	Remote misoperation	Physical Vandalism	Remote misoperation	Remote misoperation	Autonomous malware
Rem targeted ransomware	Remote shutdown	Drop malware	Erase hard drives	Erase hard drives	Sleeper malware
Ransomware	Vandalism – delete files	Remote misoperation	Remote shutdown	Remote shutdown	Remote misoperation
Virus triggers shutdown	Drop malware	Remote shutdown	Embarrass Business	Sleeper malware	Erase hard drives
Organized Crime	IT Insider	ICS Insider	Hacktivist	Intelligence Agency	Military

Upgrade to Next-Gen Firewall? No Change

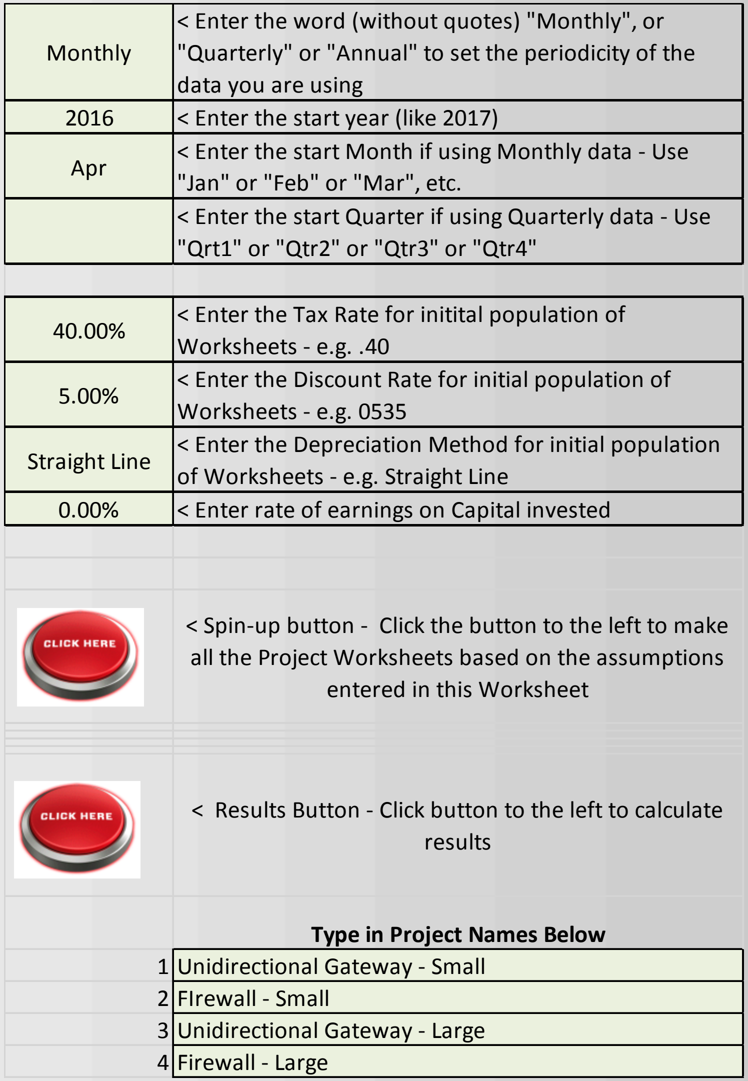
Disable safeties	Disable safeties	Local misoperation	Disable safeties	Disable safeties	Compromised insider
Rem targeted misoperation	Remote misoperation	Physical Vandalism	Remote misoperation	Remote misoperation	Autonomous malware
Rem targeted ransomware	Remote shutdown	Drop malware	Erase hard drives	Erase hard drives	Sleeper malware
Ransomware	Vandalism – delete files	Remote misoperation	Remote shutdown	Remote shutdown	Remote misoperation
Virus triggers shutdown	Drop malware	Remote shutdown	Embarrass Business	Sleeper malware	Erase hard drives
Organized Crime	IT Insider	ICS Insider	Hacktivist	Intelligence Agency	Military

Unidirectional Security Is Strong Security

Organized Crime	IT Insider	ICS Insider	Hacktivist	Intelligence Agency	Military
Disable safeties	Disable safeties	Local misoperation	Disable safeties	Disable safeties	Compromised insider
Rem targeted misoperation	Remote misoperation	Physical Vandalism	Remote misoperation	Remote misoperation	Autonomous malware
Rem targeted ransomware	Remote shutdown	Drop malware	Erase hard drives	Erase hard drives	Sleeper malware
Ransomware	Vandalism – delete files	Remote misoperation	Remote shutdown	Remote shutdown	Remote misoperation
Virus triggers shutdown	Drop malware	Remote shutdown	Embarrass Business	Sleeper malware	Erase hard drives

Maximum Security Yields Additional Savings

- Net present value = aggregate lifetime costs up front as if they were a single purchase – applying interest rate discounts
- Public NPV calculator spreadsheet can be applied to firewall cost numbers



Monthly	< Enter the word (without quotes) "Monthly", or "Quarterly" or "Annual" to set the periodicity of the data you are using
2016	< Enter the start year (like 2017)
Apr	< Enter the start Month if using Monthly data - Use "Jan" or "Feb" or "Mar", etc.
	< Enter the start Quarter if using Quarterly data - Use "Qrt1" or "Qtr2" or "Qtr3" or "Qtr4"
40.00%	< Enter the Tax Rate for initital population of Worksheets - e.g. .40
5.00%	< Enter the Discount Rate for initial population of Worksheets - e.g. 0535
Straight Line	< Enter the Depreciation Method for initial population of Worksheets - e.g. Straight Line
0.00%	< Enter rate of earnings on Capital invested
CLICK HERE	< Spin-up button - Click the button to the left to make all the Project Worksheets based on the assumptions entered in this Worksheet
CLICK HERE	< Results Button - Click button to the left to calculate results
	Type in Project Names Below
1	Unidirectional Gateway - Small
2	FIrewall - Small
3	Unidirectional Gateway - Large
4	Firewall - Large

Net Present Value Calculator Shows Cost Savings

Example firewall costs

		2016	2016	2016	2016	2016	2016	2016	2016	2016
Expense Section		Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec
Firewall suport/signature cost		1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667
Routine Firewall Management		3000	3000	3000	3000	3000	3000	3000	3000	3000
Other Firewall Management		1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667	1666.667
NIDS Support/SIgnature Cost		583.3333	583.3333	583.3333	583.3333	583.3333	583.3333	583.3333	583.3333	583.3333
NIDS Management		3000	3000	3000	3000	3000	3000	3000	3000	3000
Remote Access Operations		3750	3750	3750	3750	3750	3750	3750	3750	3750
Major Incidents		833.3333	833.3333	833.3333	833.3333	833.3333	833.3333	833.3333	833.3333	833.3333
Routine Incidents		2083.333	2083.333	2083.333	2083.333	2083.333	2083.333	2083.333	2083.333	2083.333
Insiders / Errors / Omissions		1250	1250	1250	1250	1250	1250	1250	1250	1250

NPV Results

Discounted Cash Flows		2016	2017	2018	2019	2020	2021	2022	2023
Project Names below:	PVDCF V	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov
Unidirectional Gateway - Small	76,747	50,833	498	496	494	492	490	488	486
FIrewall - Small	341,683	20,125	6,091	6,067	6,044	6,020	5,997	5,973	5,950
Unidirectional Gateway - Large	383,737	254,167	2,490	2,480	2,470	2,460	2,450	2,440	2,430
Firewall - Large	990,483	78,333	17,359	17,289	17,219	17,149	17,079	17,010	16,941

Unidirectional Gateways have lower lifecycle costs than firewalls

Strong Security – An Idea Whose Time Has Come

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC CIP V5 exempts unidirectionally-protected sites **from over 30% of requirements**

ICS-CERT
INDUSTRIAL CONTROL SYSTEMS CYBER EMERGENCY RESPONSE TEAM

DHS recommends unidirectional gateways in **security assessments** (ICS CERT)

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

NIST – gateways are **used in guarantee-ing protection** of critical systems (NIST 800-82)

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION • ANSSI •

ANSSI Cybersecurity for ICS – **many requirements for hardware-enforced unidirectionality**

enisa
European Network and Information Security Agency

ENISA - unidirectional gateways provide **better protection than firewalls**

ISA
IEC International Electrotechnical Commission

Unidirectional gateways – **limit the propagation of malicious code** (ISA SP-99-3-3 / IEC 62443-3-3)

Maximizing Network Security Is Good Business

- Maximum security architecture dramatically reduces CIP V5 compliance costs with Medium Impact ERC exemptions
- Unidirectional CIP V5 segmentation of generating yields dramatic compliance and cost-of-cyber risk reductions
- Attack modelling makes security benefits of maximum security unidirectional network architecture clear to senior decision-makers
- Net present value modelling demonstrates hidden costs of firewalled network architectures

NERC CIP program costs are naturally reduced when strong, unidirectional security is deployed

For articles & whitepapers to dig deeper on these topics: andrew.ginter@waterfall-security.com

Questions

Thank You!

WATERFALL®
Stronger Than Firewalls

ENERGYSEC
THE NATIONAL ENERGY SECTOR
CYBER SECURITY ORGANIZATION

Andrew Ginter
andrew.ginter@waterfall-security.com
www.waterfall-security.com

Steve Parker
steve@energysec.org

Karl Perman
karl@energysec.org
www.energysec.org