Unified Threat Management

Joel M Snyder
Senior Partner
Opus One
jms@opus1.com

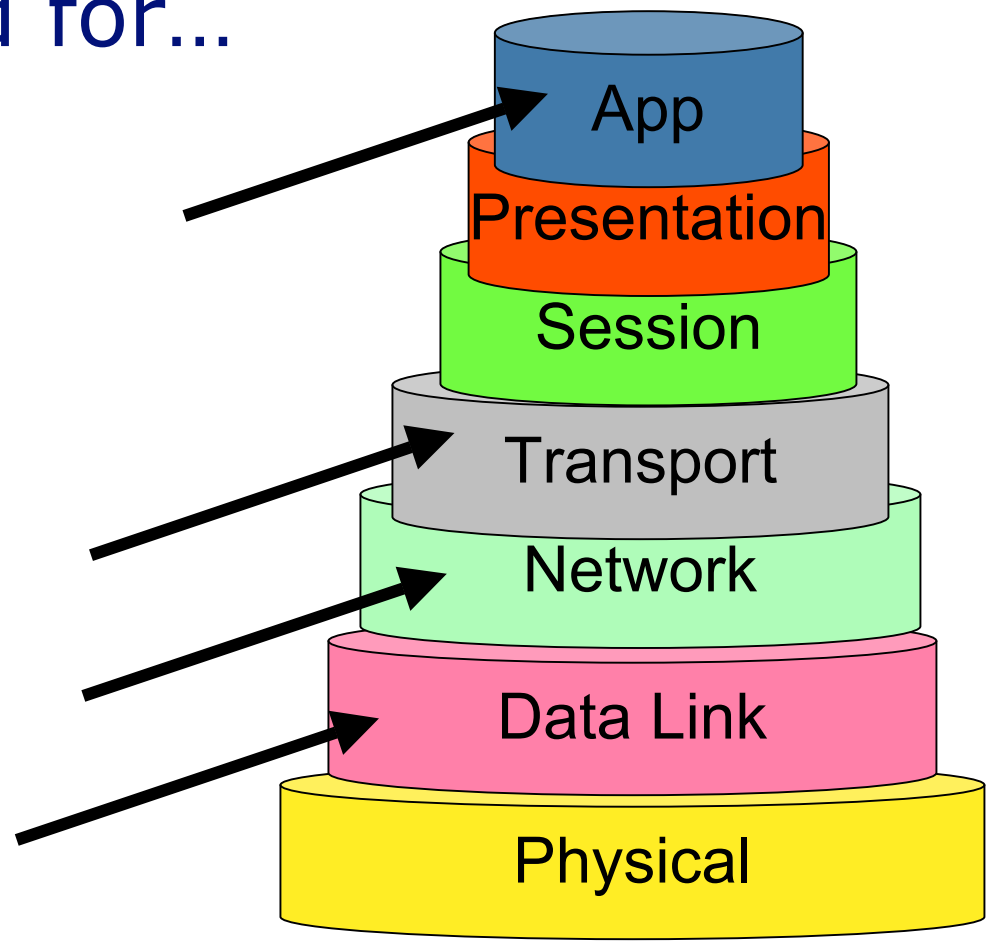
Agenda: Unified Threat Management

- **What is it?**
- **UTM Features and where you should use them**
- **Performance and UTM**
- **Cost and UTM**

What is UTM?
Why would you want to use UTM?

UTM is a buzzword for…

- **"threat mitigation we stuck in the firewall"**
- **"whatever new thing that we didn't used to do that we do now"**
  - **For a price, usually**



UTM can cover many bases

Anti-Spam

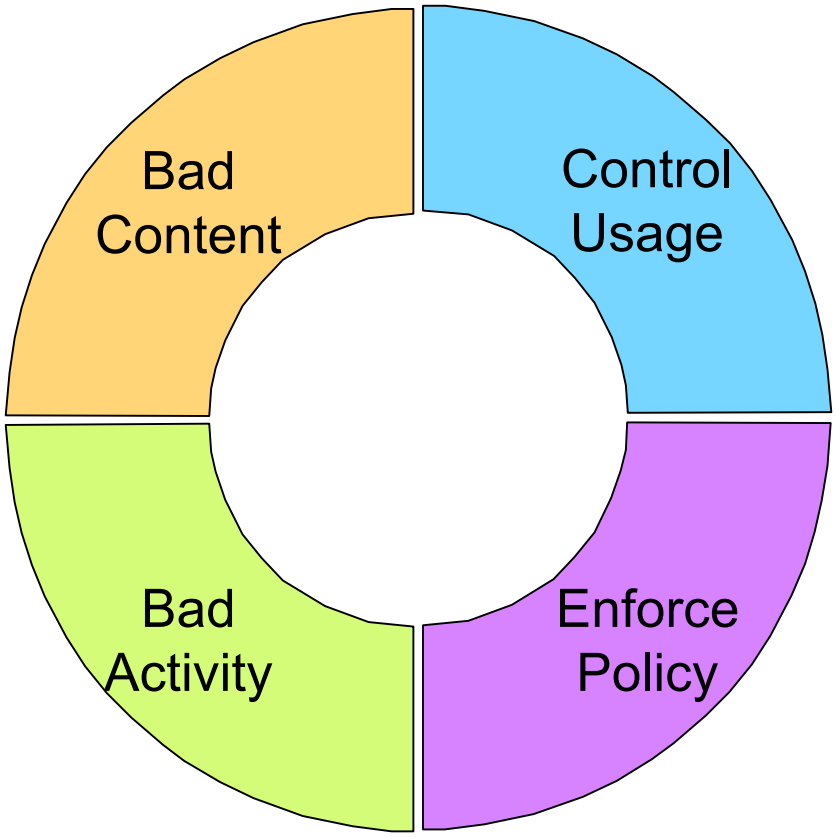
Anti-Virus

Anti-Spyware

Anti-Phishing

Intrusion Prevention

DoS/DDoS Mitigation



Content Filtering

Application Blocking

Bandwidth Management

Regulatory Logging/ Blocking

UTM has taken over the firewall industry

Current Vendors Include:

- **Check Point**
- **Cisco Systems**
- **FortiNet**
- **IBM/ISS**
- **Juniper/NetScreen**
- **Secure Computing**
- **SonicWALL**
- **Symantec**
- **Untangle**
- **WatchGuard**
- **ZyXel**

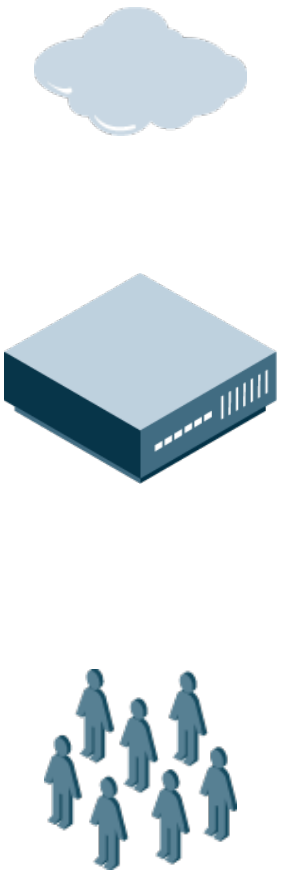
Features Include:

- **Firewall**
- **VPN**
- **Anti-Virus**
- **Anti-Spam**
- **Anti-Spyware**
- **Anti-Phishing**
- **Bandwidth Management**
- **IPS/IDS**
- **Content Filtering**
- **Web Proxy**

UTM is an alternative to the common approach to perimeter security

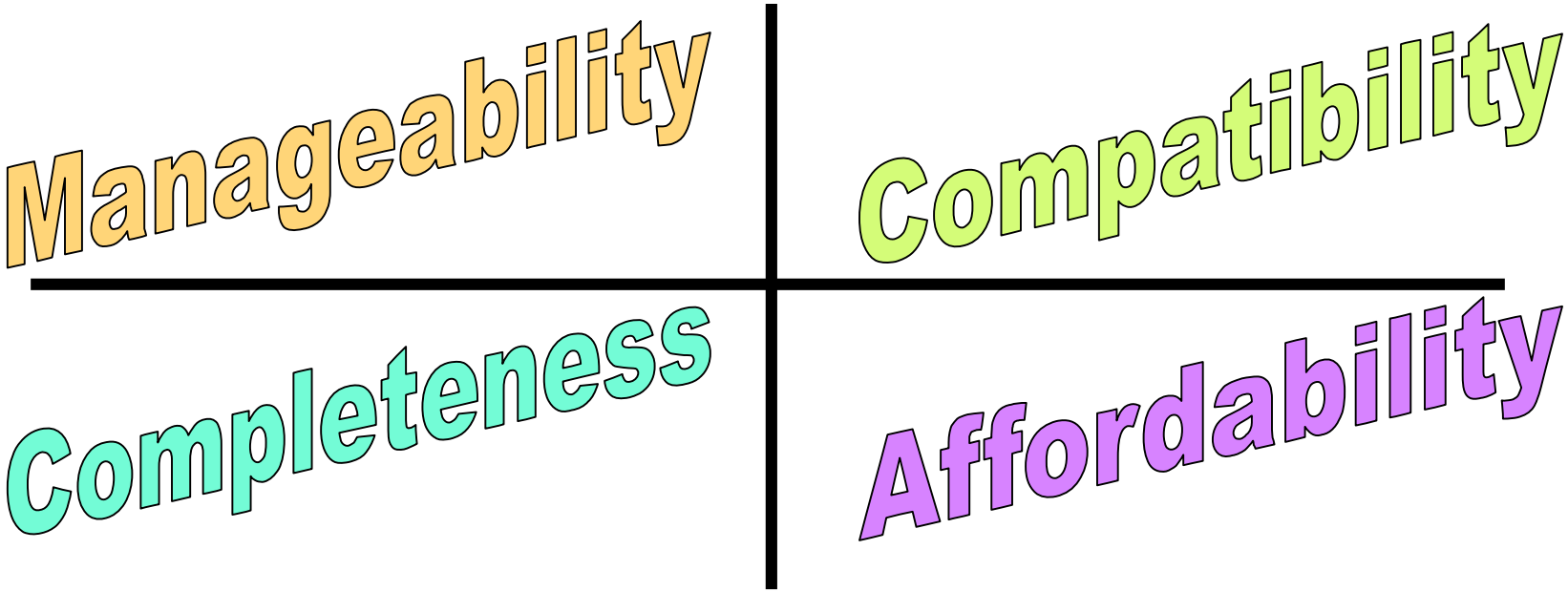
Rack'em and Stack'em

UTM



Arguments for UTM vary depending on your environment

In the SMB space, four arguments push UTM

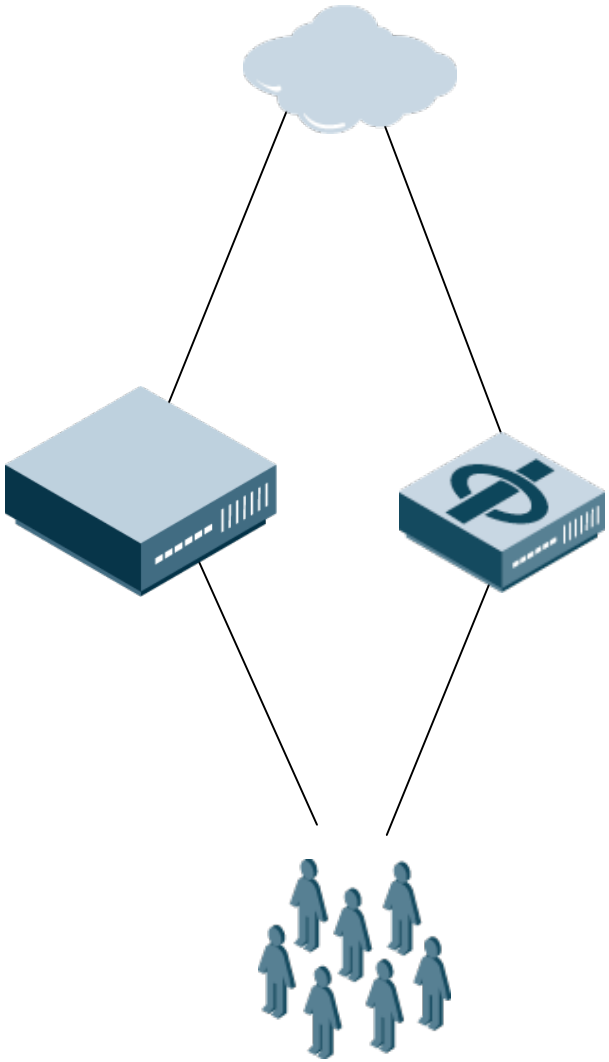


In the Enterprise Network, UTM has a very different justification

Criteria	Notes
Cost	Long-term costs for UTM will likely be lower than individual point solutions
Performance	By intelligently routing traffic to different engines, performance of a single large box can exceed multiple small boxes
Complexity	High Availability and Scalability are dramatically simplified in UTM
Management	A single management interface reduces the possibility of mistakes
Flexibility	Ability to bring security services in and out of the equation quickly supports threat response requirements best

Of course, neither strategy excludes the other

- **You may want to do a mix-and-match solution because**
  - **You have different management responsibilities (*e.g.,* email versus network layer)**
  - **You have audit requirements (*e.g.,* compliance versus security)**
  - **You have random requirements that aren't met by a single product (*e.g.,* box must be blue and have a prime number of fans)**



Which parts of UTM are best?
Which ones should I use?
What will it cost me?
What are key tactics on UTM?

Not every function in a UTM firewall offers the same level of security

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging
Regulatory Compliance

Let's run through them to make some general observations.

Start with:

The UTM/no-UTM decision is often a budget and appropriate fit one!

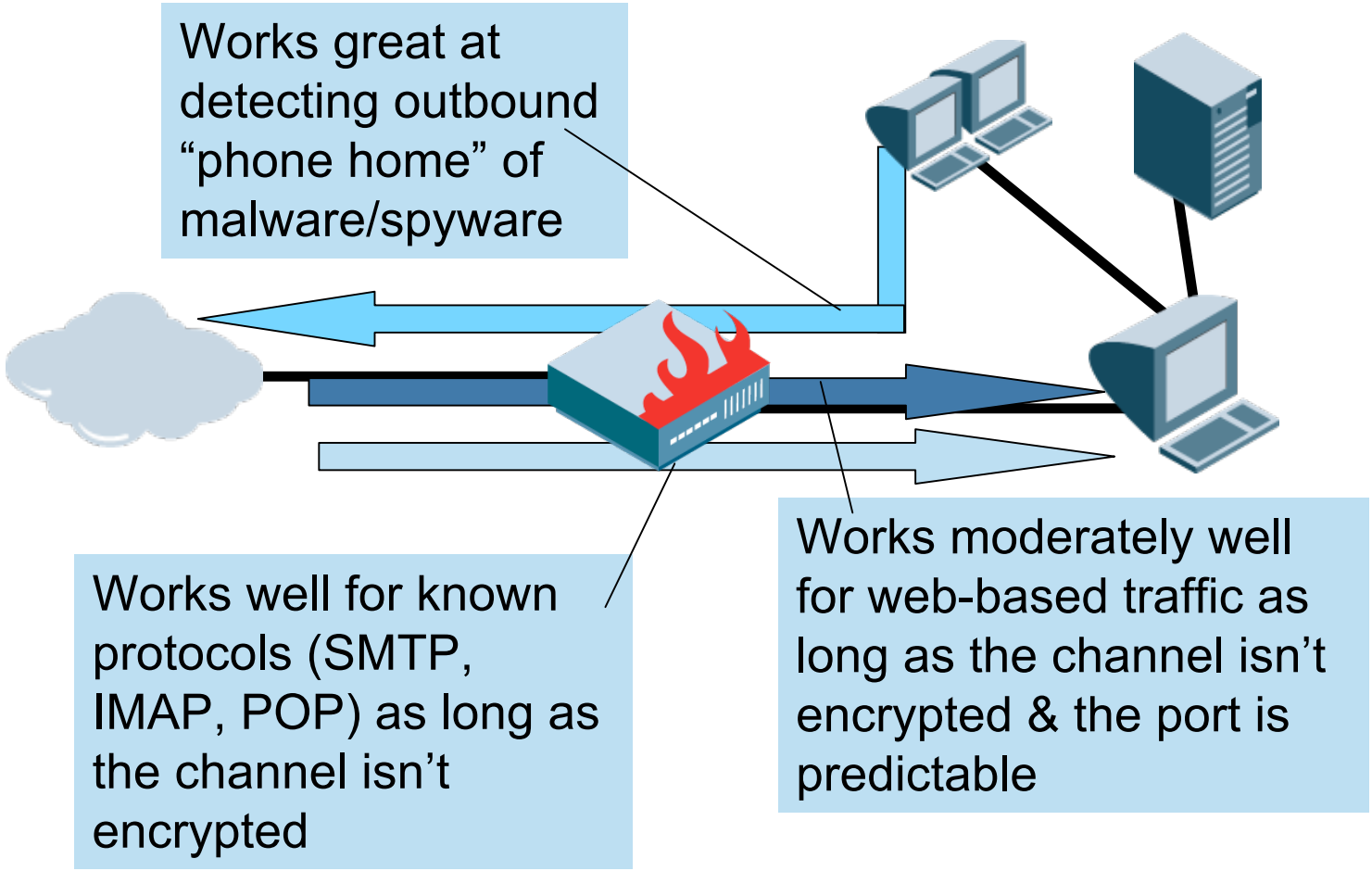
Anti-spam/Anti-phishing with UTM is not a complete package

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging
Regulatory Compliance

UTM	Edge Email Security Device
Blacklist IP-based filtering **Simple DCC or content-based anti-spam**	**Reputation-based IP filtering** **Powerful signature/ heuristic-based anti-spam** **End User Quarantine** **Per-user settings** **Greater control, reporting**

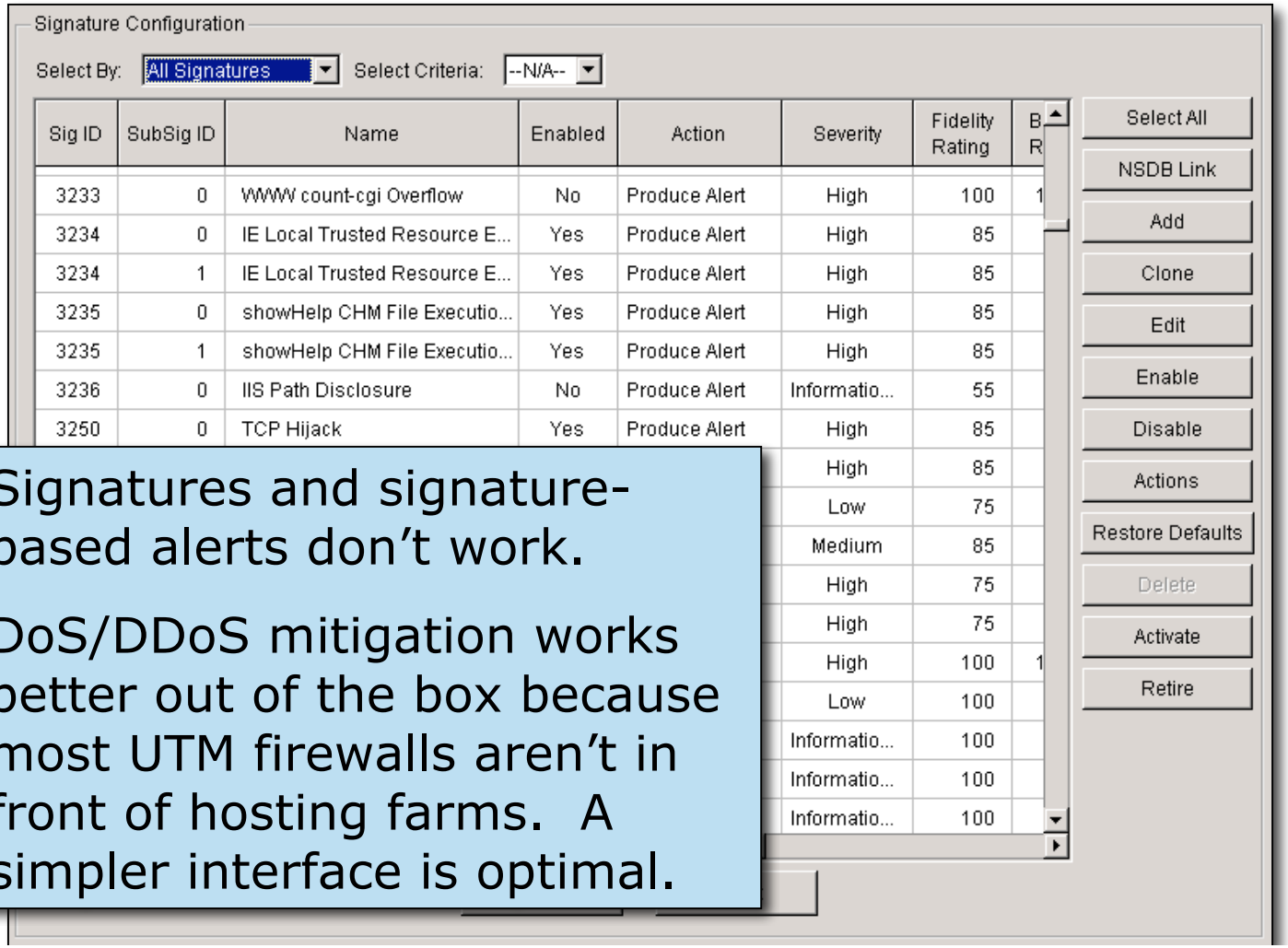
Anti-Virus and Anti-Spyware are the most common UTM features

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging
Regulatory Compliance



With IPS, the problem isn't the technology but the interface

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging
Regulatory Compliance



Signatures and signature-based alerts don't work.

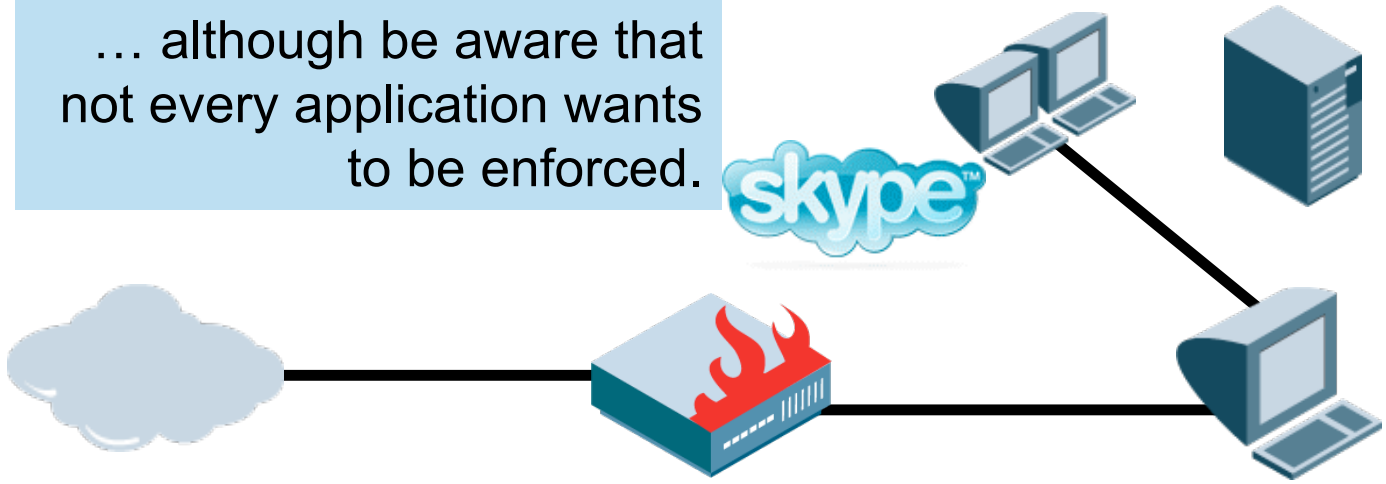
DoS/DDoS mitigation works better out of the box because most UTM firewalls aren't in front of hosting farms. A simpler interface is optimal.

Content Filtering and Application Blocking are "sweet spots" for firewalls

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging
Regulatory Compliance

As a choke-point, firewalls are perfectly situated to enforce policy…

… although be aware that not every application wants to be enforced.



With content filtering, a 90% solution is generally acceptable.

Logging and Compliance *require* more than a UTM firewall

Anti-Spam
Anti-Virus
Anti-Spyware
Anti-Phishing
Intrusion Prevention
DoS/DDoS Mitigation
Content Filtering
Application Blocking
Logging and Auditing
Regulatory Logging & Compliance

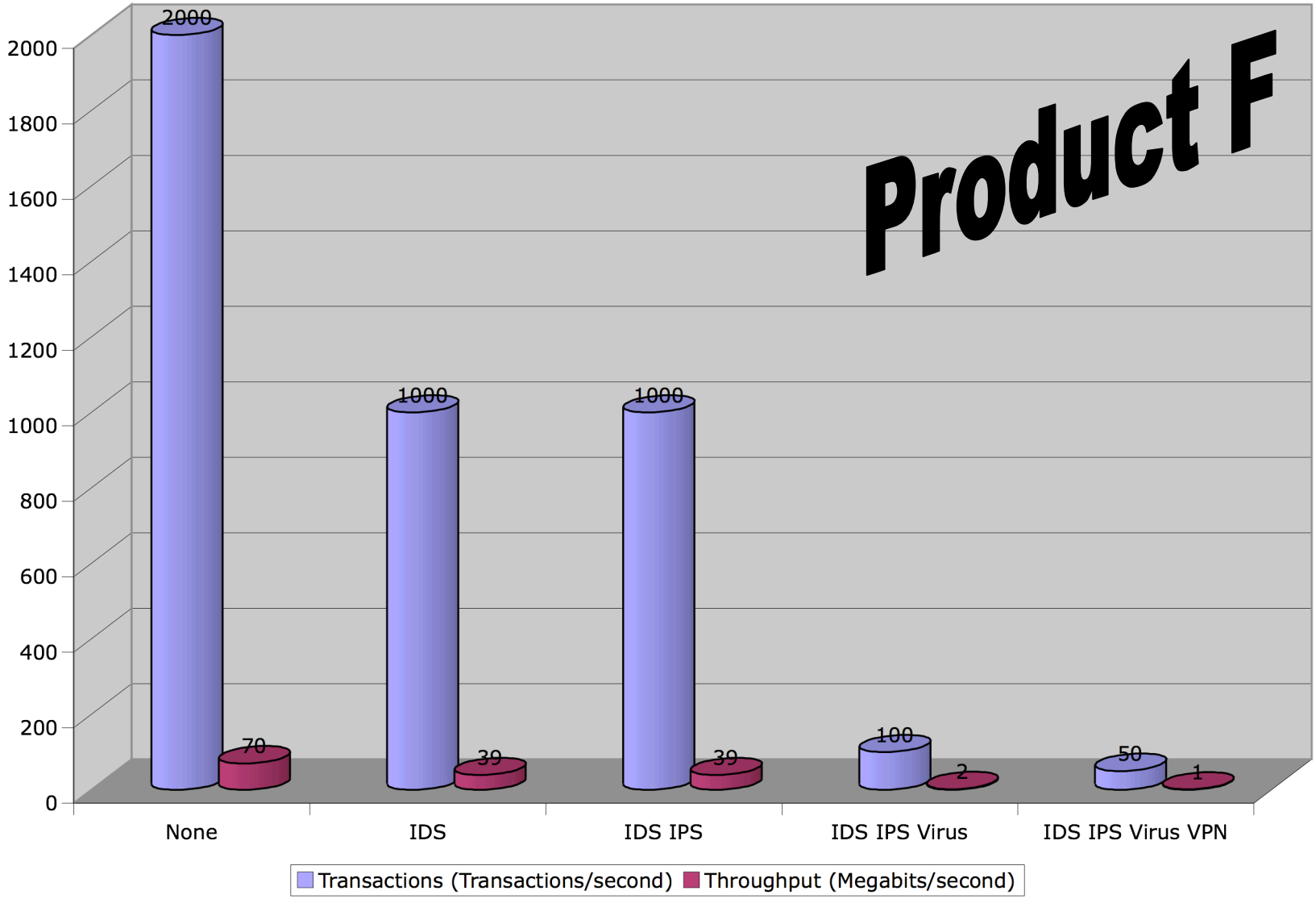
Regime	Goal	How IT Helps?
GLBA	**Protection of private financial information**	**More firewalls; leak protectors**
SOX	**Financial reporting integrity**	**More disk**
HIPAA	**Health information privacy and control**	**More firewalls; leak protectors**
SEC 17A-4	**Support of audit process**	**More disk**
California SB1386	**Disclosure when a privacy breach occurs**	**More firewalls**
Basel II	**Promoting financial stability**	**More firewalls; disk**
EU Data Protection	**Personal information integrity**	**More firewalls; leak protectors**

Best Practices for UTM

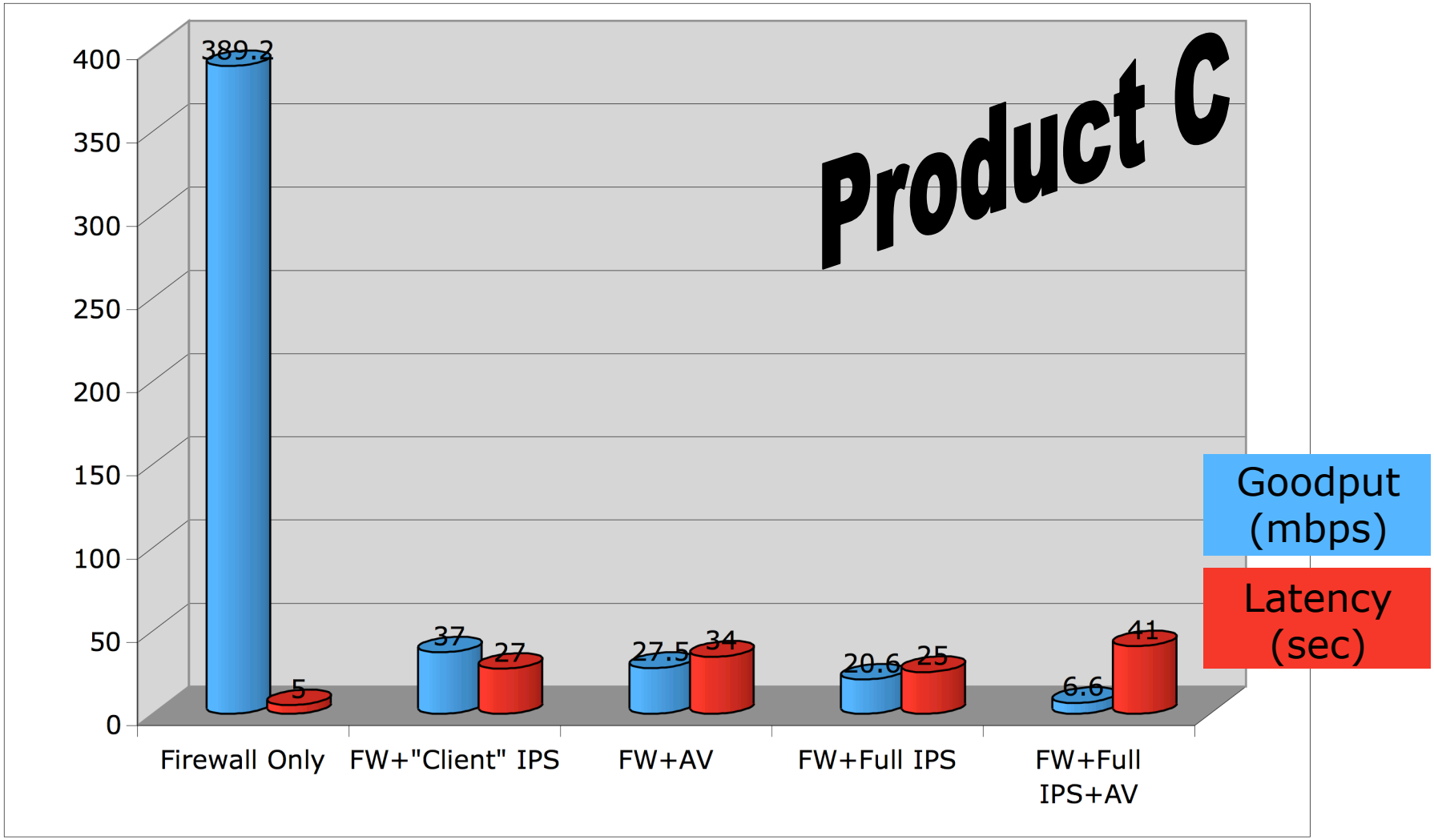
Use firewall + UTM where it fits perfectly	**DDoS mitigation, application control, bandwidth management, content filtering**
Use UTM to backstop better technologies	**Anti-virus, anti-spyware**
Don't use UTM where it doesn't work well	**Anti-spam, anti-phishing**
Don't use technologies you don't understand or won't manage	**IPS, IDS**
Let your budget override everything	**Imperfect security is better than no security**

UTM Performance: Nothing is Free

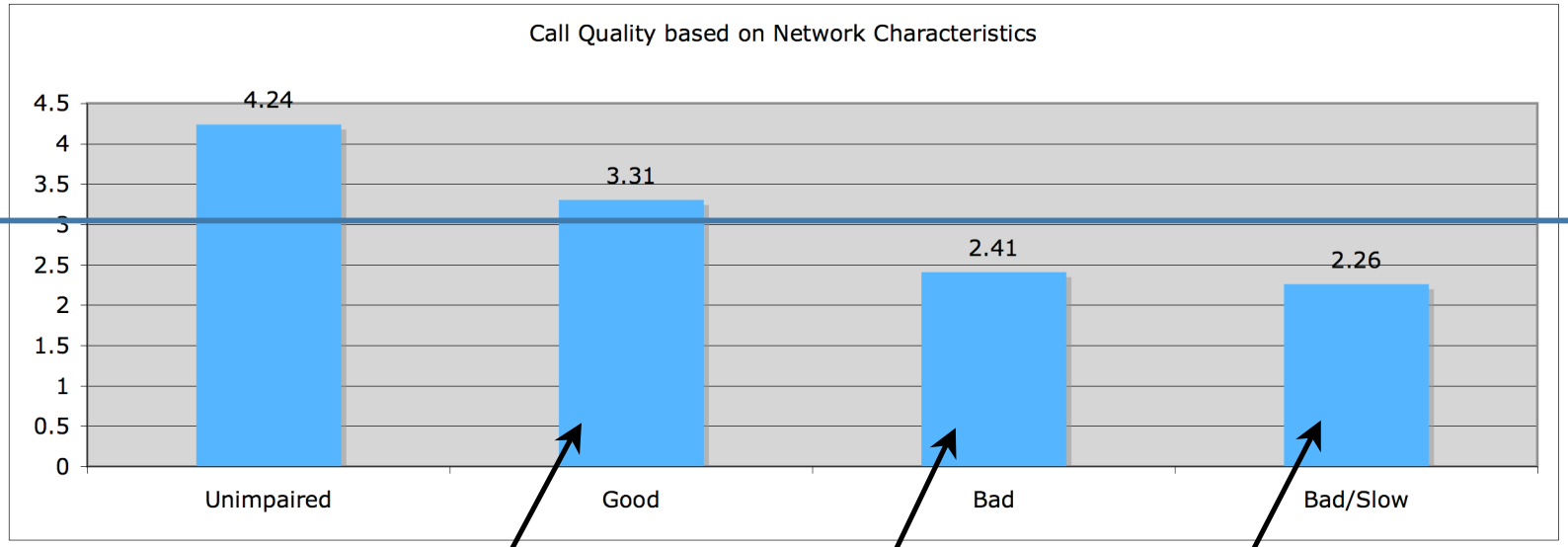
UTM Performance: Nothing is Free



Performance hit is no anomaly



Goodput is not the most important metric for a firewall



Added moderate latency

Added latency and loss

Added latency, loss, and bandwidth cap

UTM has benefits, and it has costs

UTM Benefits	UTM Costs
• Reduces number of boxes you have to buy • Reduces amount of un-coordinated management • Ideally positioned (bottleneck) for Internet-facing security • Allows you to incrementally add security without complexity	• System performance can be dramatically affected • "Single Choice" may be wrong choice for your network • Some UTM features are in for check-list purposes, and not for security purposes • Subscription costs need to be budgeted

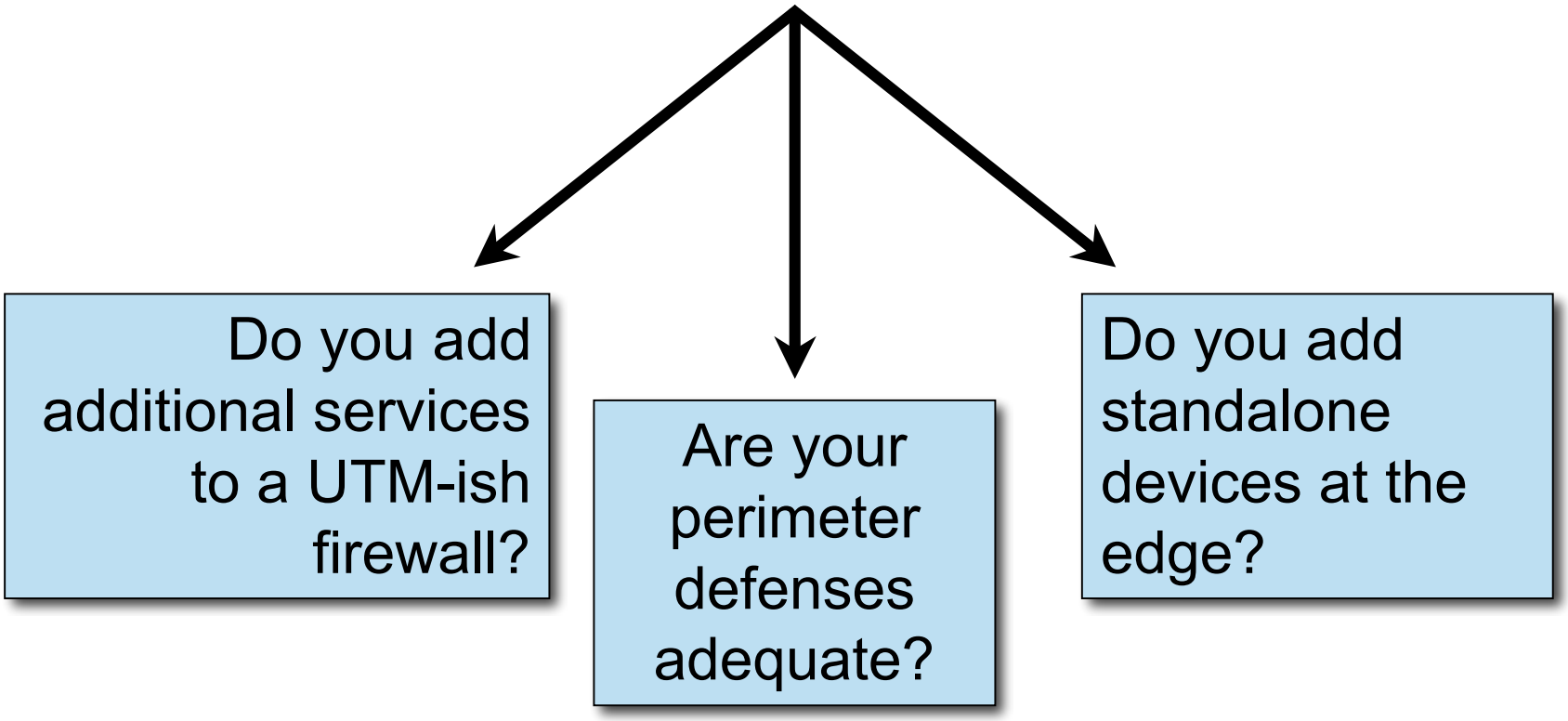
Four Key Tactics for UTMs

- **The Devil Is In The Details**
  - **Understand exactly what features of perimeter defense you need. If you don't need it, don't ask for it.**
- **Do What Makes Sense**
  - **Natural consolidation is a good thing. Forcing consolidation is a bad strategy.**
- **Nothing is Free**
  - **Adding security services to your network at any point will cost you time, money, and reliability. If you don't budget for it, how are you going to pay for it?**
- **A Strong Perimeter is a Good Thing**
  - **But a deep defense is a better thing. Don't let money spent on the edge deceive you.**

How do I make a business case for UTM?
Will UTM save me money, really?

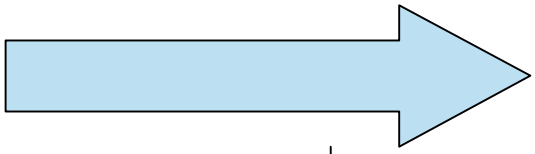
Perimeter Intrusion Defense is something you already have

- **The question is: how do we grow perimeter security? Should we use UTM or not?**



How a Normal Business Decision is Supposed to be Made

Business Requirements and Needs



IT or MIS Project, Action, or Service

"Customers need to be able to see the status of orders, including shipping and tracking information."

Project: Web-based portal into SAP to show order status; link to UPS via XML for shipping information

The problem with security it that it doesn't solve direct requirements

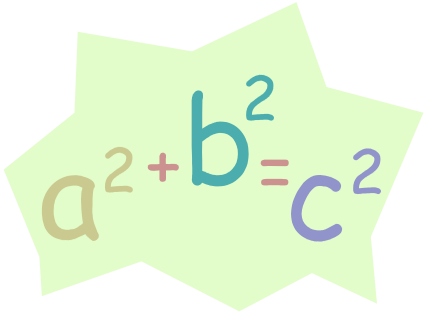
Business Requirements and Needs

→

IT or MIS Project, Action, or Service

???

<u>Project:</u> Upgrade our existing firewall to UTM version to add Intrusion Prevention System on Internet-facing links



So most security people build frameworks…

SLE = Single Loss Expectancy
EF = Exposure Factor (0-100%)
ALE = Annual Loss Expectancy
ARO = Annual Rate of Occurrence (0-100%)

Identify assets and define their value

Identify threats to assets

Calculate
SLE = (EF x Value) + Downtime

Calculate
$ALE_{before} = ARO_{before} * SLE_{before}$

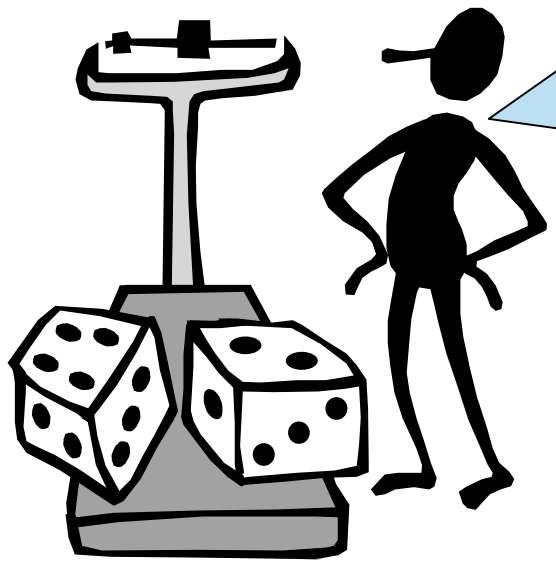
Figure out a solution that mitigates risk

Change EF, ALE, and ARO

Calculate
$ALE_{after} = ARO_{after} * SLE_{after}$

Compare ALE_{before} with ALE_{after}

Even if the numbers are largely bogus, you can ask yourself…



Is the amount of money I am proposing to spend LESS or MORE than the change in ALE?

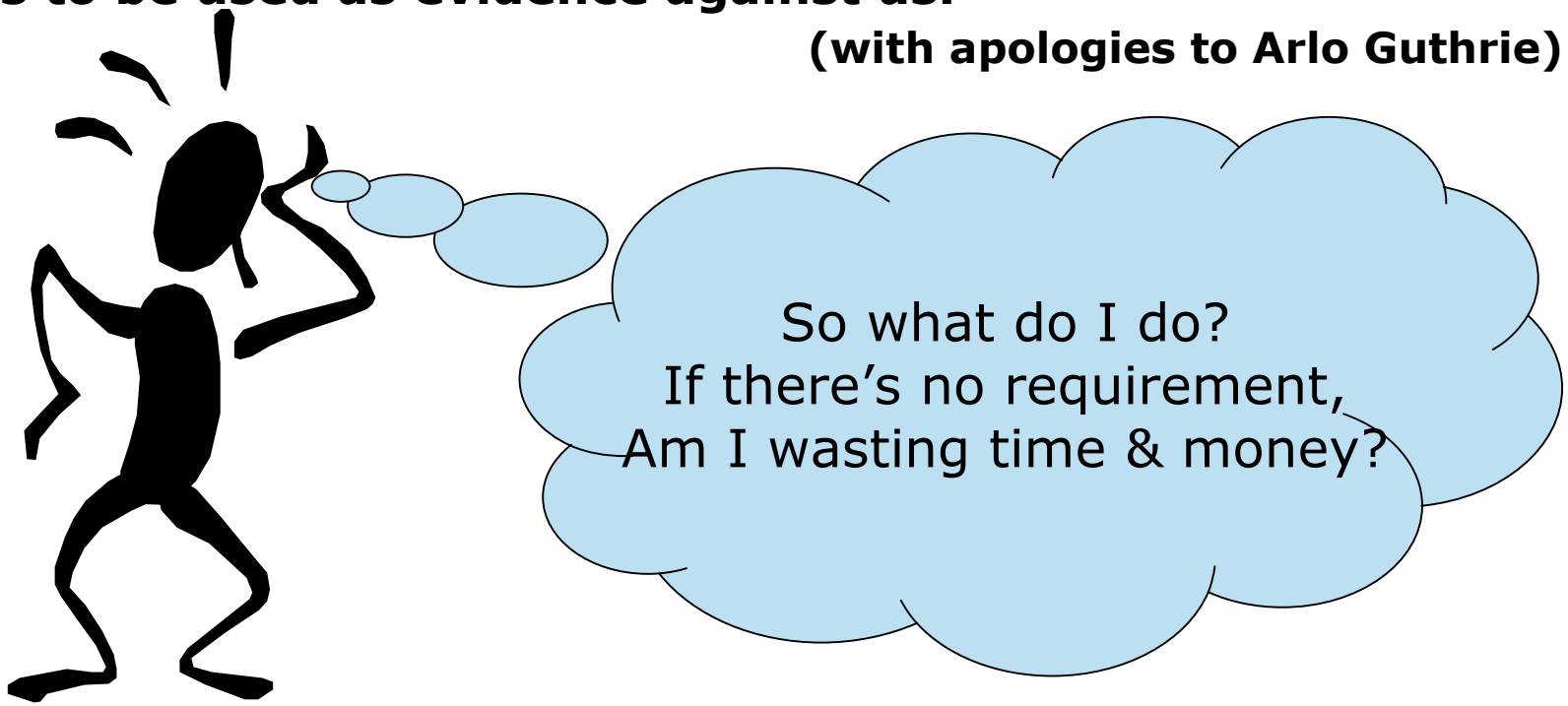
Compare ALE_{before} with ALE_{after}

$$\Delta = ALE_{before} - ALE_{after}$$

But your typical CxO doesn't want to see the framework

- **"The CIO wasn't going to look at the twenty seven eight-by-ten color glossy pictures with the circles and arrows and a paragraph on the back of each one explaining what each one was to be used as evidence against us."**

(with apologies to Arlo Guthrie)



You can fall back to the Security Manager's Best Friend

- **The Fear, Uncertainty, and Doubt Strategy**

Find out what newspaper the CxO reads

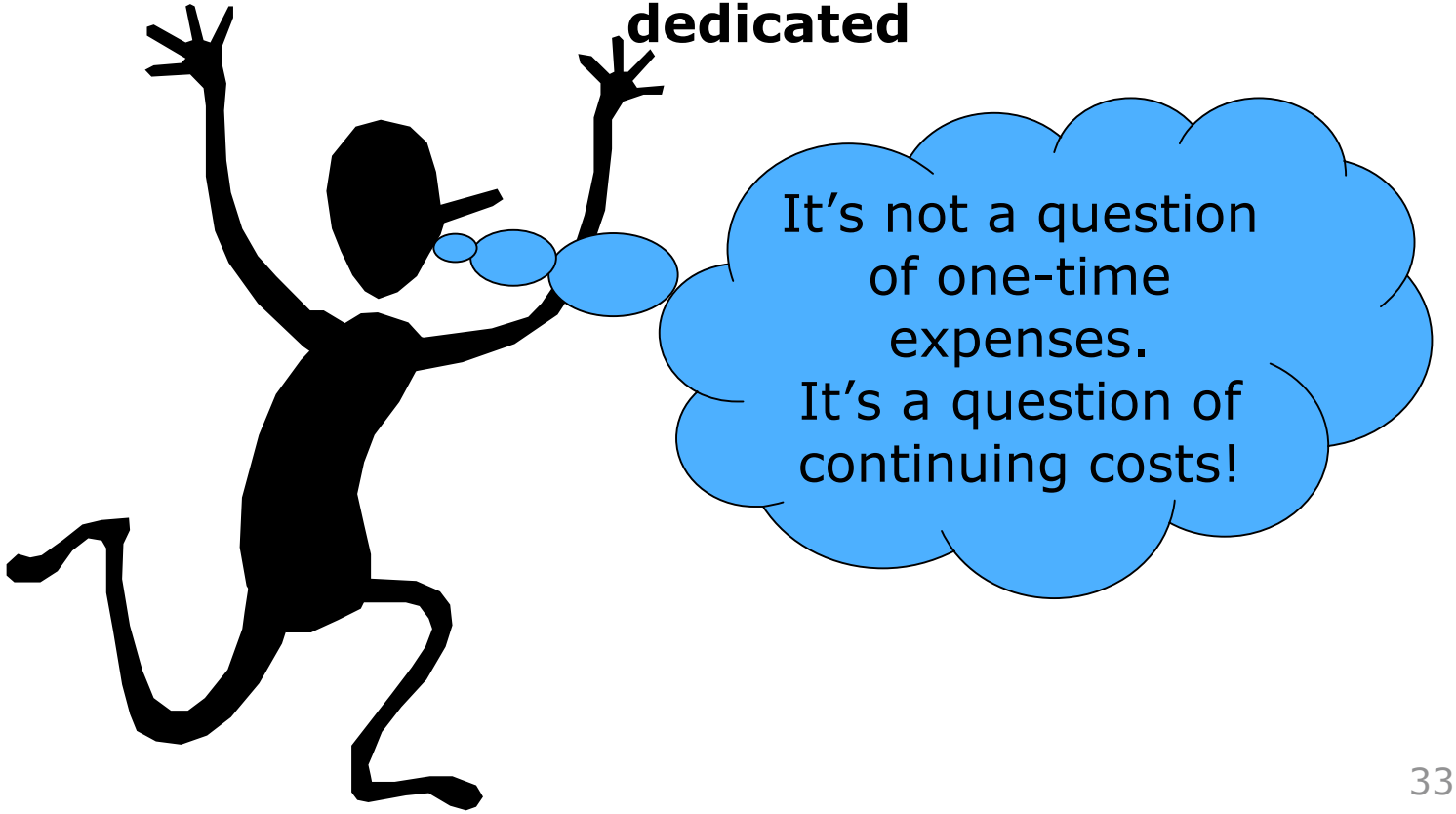
Get a Subscription and Read It
(Hint: you may have to touch paper to do this)

Wait until there is a story about some awful security thing happening to someone, somewhere

Run into CxO's office with unsigned purchase requisition for random piece of security SW/HW. Tell him/her this will keep them out of the newspaper.

When you add these new technologies, there are OpEx costs

- **UTM technology is moving from a CapEx model to an OpEx model**
- **Adding security services adds management costs whether UTM or dedicated**



For example, let's suppose you like the ZyXel ZyWALL UTM 70 firewall

Capital Cost: $1,588.00

- **1 Year: Anti-Virus and Intrusion Prevention: $362**
- **1 Year: Anti-Spam: $202**
- **1 Year: Content Filtering: $299**

Capital:
$1,588.00

Security Services:
$863.00

But wait, there's more…

Hardware maintenance tasks

- Firewall configuration management, @ 24 hours/year
- Periodic Software Updates, @ 12 hours/year

Software maintenance tasks

- Anti-virus management, @ 12 hours/year
- Intrusion Prevention management, @ 48 hours/year
- Content Filtering management, @ 24 hours/year
- Anti-spam management, @ 48 hours/year

Management Time: 168 hours/year, or about $6,500.00

Capital: $1,588.00

Security Services: $863.00

How about the SonicWALL PRO 2040?

Capital Cost: $1,995.00

- **1 Year: Anti-Virus and Intrusion Prevention: $695**
- **1 Year: Content Filtering: $995**

Capital:
$1,995.00

3 year Service costs:
$4,788.00

(special package deal)

How about the Netscreen SSG20?

Capital Cost: $1,100.00

- **1 Year: Anti-Virus, IPS, Content Filtering, and Anti-Spam: $700**

Capital:
$1,100.00

3 year Service costs:
$2,100.00

You can always save money using Open Source technologies

ZyXel Proposal (1 year costs)	Open Source Proposal (1 year)
• Capital: $1,588 • Support: $863 • Overhead: 168 hours, $6500	• Capital: $000 • Support: $000 • Overhead: 336 hours, $13,000
• Total: $8,951	• Total: $13,000

OK, I just put this in here as flame bait.
But the point is real: overhead costs for this technology dominate acquisition costs

All this tells us some very unpleasant things

- **It's hard to justify spending money on security, because the ROSI (Return on Security Investment) or ROI (Return on Investment)**
- **The cost for the hardware is very reasonable, but…**
- **The cost for the 'service' can add 50% to 100% to the total each year, and…**
- **Your overhead and management costs are a continuing burden**

Tips and Hints: The Business Case for UTM Security

- **DO** make the calculation of costs and expected benefits for any intrusion defense.
  - **Learning IPS might be a lot of fun, but if it doesn't bring <u>enough</u> value, maybe it's not right.**
- **DO NOT** fail to budget for support and subscriptions. UTM firewalls without updates are doorstops.
- **DO** prioritize based on your requirements and risks. **DO NOT** pick services because they came with the UTM firewall you already bought.
- **DO NOT** depend on FUD to sell security. But **DO** take advantage of it when opportunity presents itself.

Thanks!

Joel Snyder
Senior Partner
Opus One
jms@opus1.com

OPUS one