SANS

SEC530: Defensible Security Architecture

Eric Conrad (GSE # 13) and Justin Henderson (GSE # 108)
@eric_conrad and @SecurityMapper

About Us

Justin Henderson | @SecurityMapper

- SEC555/SEC530/SEC455 Author & Instructor
- GIAC GSE # 108, Cyber Guardian Blue and Red
- 60 industry certifications

Eric Conrad | @eric_conrad

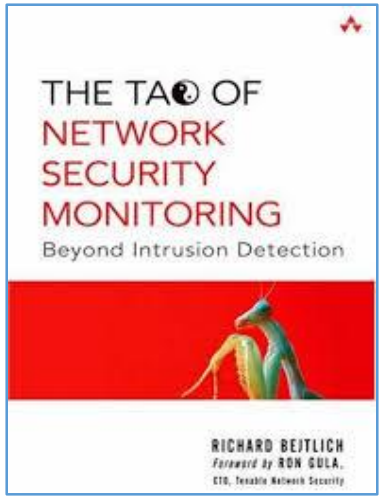
- MGT414/SEC511/SEC530/SEC542 Author & Instructor
- GIAC GSE # 13, Cyber Guardian Red
- SANS Faculty Fellow

Where We Came From

- Perimeter defense is "a sort of crunchy shell around a soft, chewy center."[1]
  - Bill Cheswick (1990), describing the first internet gateways (proxy firewalls)
- This was a reasonable design in 1990
- We have come a long way since then, but many organizations still have this "candy bar" design
  - Hard on the outside, soft on the inside
  - Flat networks with little to no internal segmentation
  - A hardened perimeter, but many weaker/unpatched internal systems

Defensible Security Architecture

- The term "Defensible Networks" was coined by Richard Bejtlich in *The Tao of Network Security Monitoring*
  - *I use the term defensible networks to describe enterprises that encourage, rather than frustrate, digital self-defense.*[1]
- Bejtlich makes these points about defensible networks:
  - *Defensible networks can be watched*
  - *Defensible networks limit an intruder's freedom to maneuver*
  - *Defensible networks offer a minimum number of services*
  - *Defensible networks can be kept current*[1]



Defensible Network Architecture 2.0

Richard Bejtlich later refined the idea of Defensible Networks, using the term Defensible Network Architecture 2.0, which he described as having the following characteristics:

- Monitored
  - Deploy IDSes and IPSes
- Inventoried
  - Know every host and application
- Controlled
  - Ingress and egress filtering
- Claimed
  - Identify owners of all systems
- Minimized
  - Reduce the attack surface
- Assessed
  - Conduct vulnerability assessments
- Current
  - Patched[1]

Case Study: NotPetya

- NotPetya is part of a family of malware based on the leaked (alleged) NSA hacking tools, including ETERNALBLUE
  - This exploit targeted Windows Server Message Block (SMB, TCP port 445) and was patched by MS17-010[1]
- This malware would typically enter an environment via SMB
  - It would then use Mimikatz to attempt to steal credentials and move laterally through a network via Microsoft PSExec and WMIC (Windows Management Instrumentation Console
  - Automated malware is now behaving like human penetration testers
- If an organization had one unpatched system and 999 patched: all 1,000 could become compromised
  - This is dependent on internet network segmentation, trust models, etc.

SEC530 Problem Solving

If perimeter security is not the answer then…

- We need to buy next-gen security products FALSE
- We need to use existing things in new ways TRUE

Example wins with solutions you likely own:

- Private VLANs
- NetFlow
- Darknet Routing
- HSTS Preloading
- Explicit Proxies
- Sender Authentication and checks
- File Classification w/controls
- WAF central policies

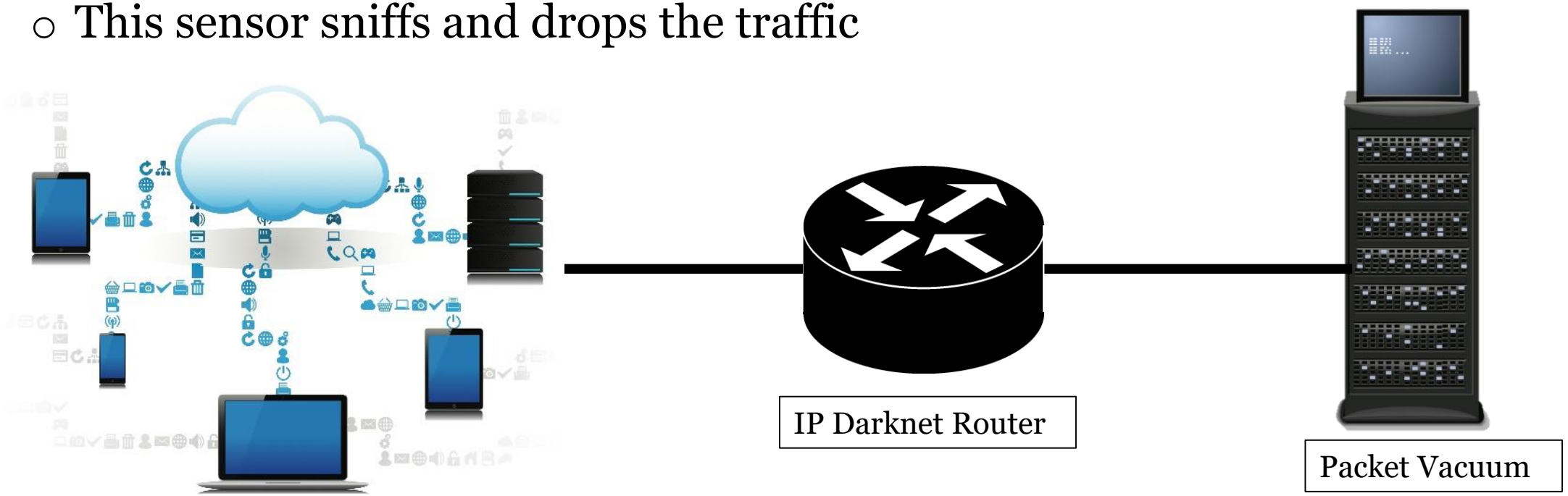
Creates defense-in-depth and complimentary capabilities

Private VLANs (PVLANs)

- Private VLANs are (usually) one of the easiest 'wins' an organization may achieve for making pivoting more difficult to an attacker
  - 'Pivoting' describes the act 'moving behind enemy lines,' when malware (or a person) moves from one compromised internal host to another host
  - Lots of malware will attempt to pivot from one client PC to another
- Many corporate wireless solutions offer 'station isolation': a client on a wireless access point may speak to the AP (which is also a switch and a router) only
  - Clients may not access other clients on the same AP
  - Station isolation is also called client isolation
- A private VLAN is the wired equivalent to wireless station isolation
  - If this makes sense for wireless clients: why not wired?

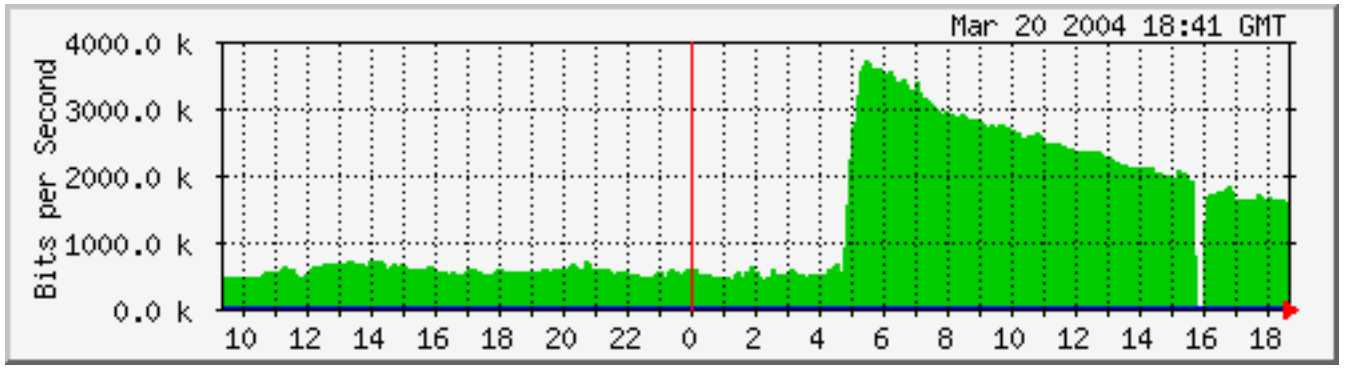
IP Darknet Architecture

- Route all IP darknet traffic to a dedicated darknet router
  - Monitor this traffic via SNMP
- That router forwards traffic to a 'packet vacuum' sensor
  - This sensor sniffs and drops the traffic



What Kind of Traffic Is Sent to an IP Darknet?

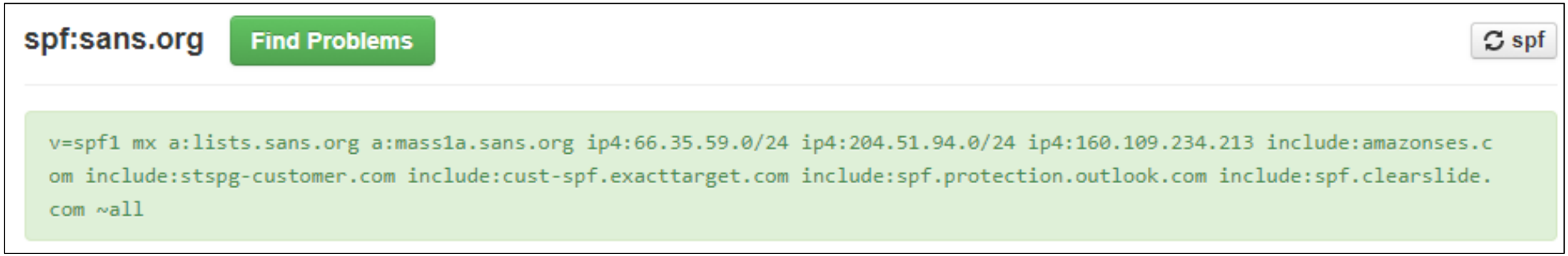
- All traffic sent to a darknet is bogus, by definition
  - There are two types of darknet traffic sources: misconfigured and/or malicious traffic
  - IP darknet monitoring can offer critical insights into misconfigured and/or malicious traffic on a network
- Team Cymru's IP Darknet monitor discovered the Witty worm[1]:



Sender Policy Framework (SPF)

DNS record validates email sent from an authorized source

- Based on authorized IP addresses
- Based on DNS domain information (A record, MX record)
- Can specify no email comes from a specific sub-domain



dnstwist[1]

Proxy can protect against cousin domains (`sec530.com`)

- Possible to add all possible domains into proxy
- Should configure to **block** or **quarantine and alert**
- Requires identifying all possible domain permutations

dnstwist calculates permutations against a given domain

- Also checks to see if any domains have been registered
- And provides additional information about the domain

Use dnstwist with scripting to handle deal with evil cousins

Know Thy Organization

A defensible architecture requires organizational awareness

- What are critical assets?
- Where are the critical assets?
- Why are they considered critical assets?
- What do these assets need to function?

Knowing the above questions allows defenses to be built

- **Network-centric** defenses build a security moat
- **Data-centric** defenses secure the treasure in the castle

Suricata

Suricata is a modern open-source IDS/NSM

- Developed by Open Information Security Foundation
- Supports snort rules and **application** identification
- Generates alerts and network metadata logs

Example signature rule:

```
alert tcp any any -> any !22 (msg:"SURICATA SSH
non-standard port"; flow:to_server; app-layer-
protocol:ssh; sid:5300001; rev:1;)
```

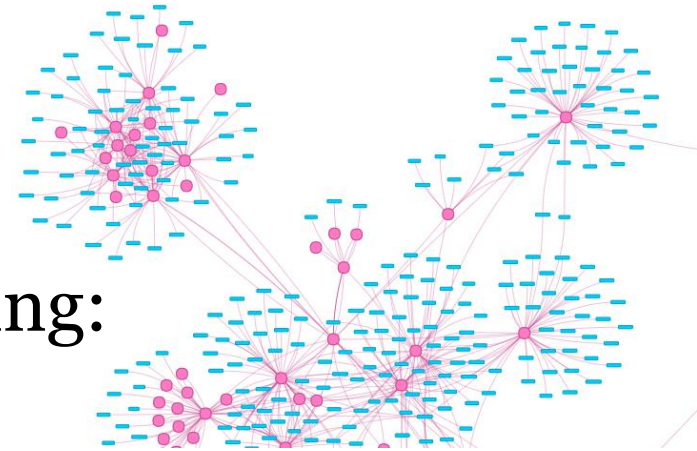
Bro

Suricata is both an IDS and NSM in that it creates logs

- Bro is built for creating logs from network traffic
- Requires sensor placement and network visibility

Network Protocols					Files	Detection
conn.log	http.log	radius.log	smb_mapping.log	syslog.log	files.log	intel.log
dce_rpc.log	irc.log	rdp.log	smtp.log	tunnel.log	pe.log	notice.log
dhcp.log	kerberos.log	rfb.log	snmp.log		x509.log	signatures.log
dnp3	modbus.log	sip.log	socks.log			traceroute.log
dns.log	mysql.log	smb_cmd.log	ssh.log			
ftp.log	ntlm.log	smb_files.log	ssl.log			

Power of Network Metadata



IDS signatures look for known bad

- Network metadata is simply data

Allows for learning the environment and identifying:

- **Abnormal events**
  - Unusual/newly observed/random domains or user-agents
- **Unauthorized assets**
  - Computer DHCP but not in Active Directory or asset system
- **Vulnerable or misconfigured assets**
  - Old operating systems or applications on the network

SSL Inspection

Security devices like NGFW or web proxies support SSL Inspection

- Functions similar to a proxy service

Security device acts as trusted CA to internal devices

- Issues certificates per site accessed
- Fixes visibility issues such as perfect forward secrecy blindness
- Requires systems to trust security device as CA

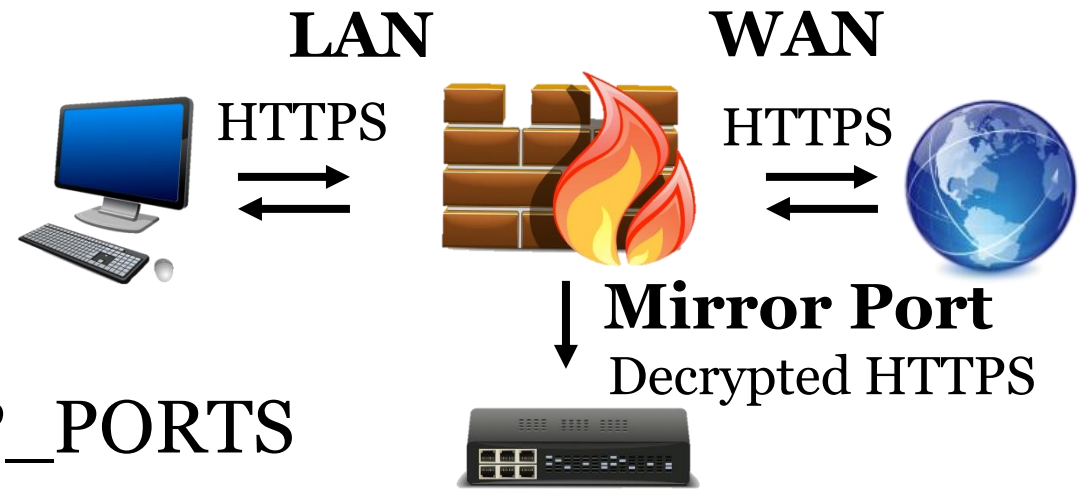
SSL Decrypt Mirror Port

Modern devices with SSL Inspection also support SSL decrypt mirroring

- Decrypted packets are mirrored out an interface
- Puts NSM/IDS back in the game

Decrypted traffic shows up with the original port such as `443`

- But reflects decrypted data
- IDS should include `443` in $HTTP_PORTS

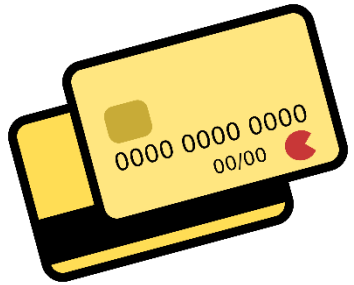


Finding Sensitive Data

Need to identify key data and where it is expected

- File servers
- Database servers
- USB drives

Expected



Probable reality

Next, is to realize where it may end up

- Laptops
- Mobile phones
- Personal USB devices

Content Discovery Script Example

Less than 40 lines of code including 10 lines of comments

- Loops through each **database**, **table**, and **column** and checks all **values**

```
Import-Module SqlServer
$server = "10.5.30.2"
$user = "SA"
$password = 'password'
$credit_card_patterns = @{visa = '4[0-9]{12}(?:[0-9]{3})?'; mastercard = '(?:5[1-5][0-9]{2}|222[1-9]|22[3-
$databases = Invoke-Sqlcmd -ServerInstance $server -Query 'select name from sys.databases WHERE name NOT I
foreach($database in $databases){
    $tables = Invoke-Sqlcmd -ServerInstance $server -Query 'SELECT table_name FROM INFORMATION_SCHEMA.TABL
    foreach($table in $tables){
        $fields = Invoke-Sqlcmd -ServerInstance $server -Query 'SELECT column_name,data_type FROM INFORMAT
        # Possible to limit field types to search
        # This example just cralws them all
        foreach($field in $fields){
            [string]$field_name = $field.column_name
            $field_values = Invoke-Sqlcmd -ServerInstance $server -Query 'SELECT $field_name FROM $table'
            foreach($field_data in $field_values){
                foreach($pattern in $credit_card_patterns.Values){
                    if($field_data -match $pattern){
                        foreach ($key in ($credit_card_patterns.GetEnumerator() | Where-Object {$_.Value -
                            $card_type = $key.name
                        }
                        Write-Host "Found possible credit card number $field_data found in $database - $ta
```

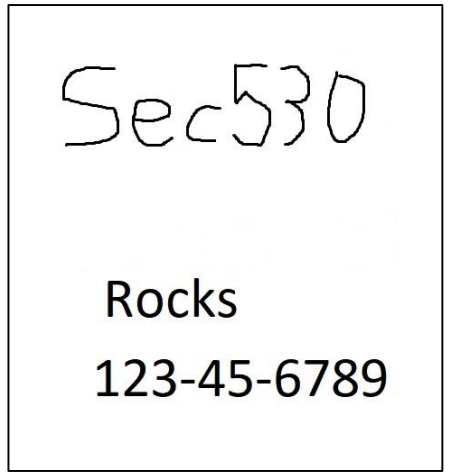
Optical Character Recognition (OCR) Integration

File classification supports OCR of TIFF (faxes and scans)

- Vendor solutions have more file support and OCR capabilities

Possible to live off the land with PowerShell

- Find certain files such as JPG
- OCR scan them looking for sensitive data
- If sensitive content found add file property
- Can be integrated into automatic classification




```
PS C:\> Export-ImageText -path C:\530\USB-content\Day4\ocr.jpg
Sec530

Rocks
123-45-6789
```

Zero Trust Architecture

Developed by Forrester's John Kindervag in 2010[1]

- Data-centric focus

Basic principles of zero trust:

- Network is always hostile
- Internal and external threats are always present
- Internal network is not sufficient to equal trusted
- Every device, user, and network flow must be proven
- Log and inspect all traffic

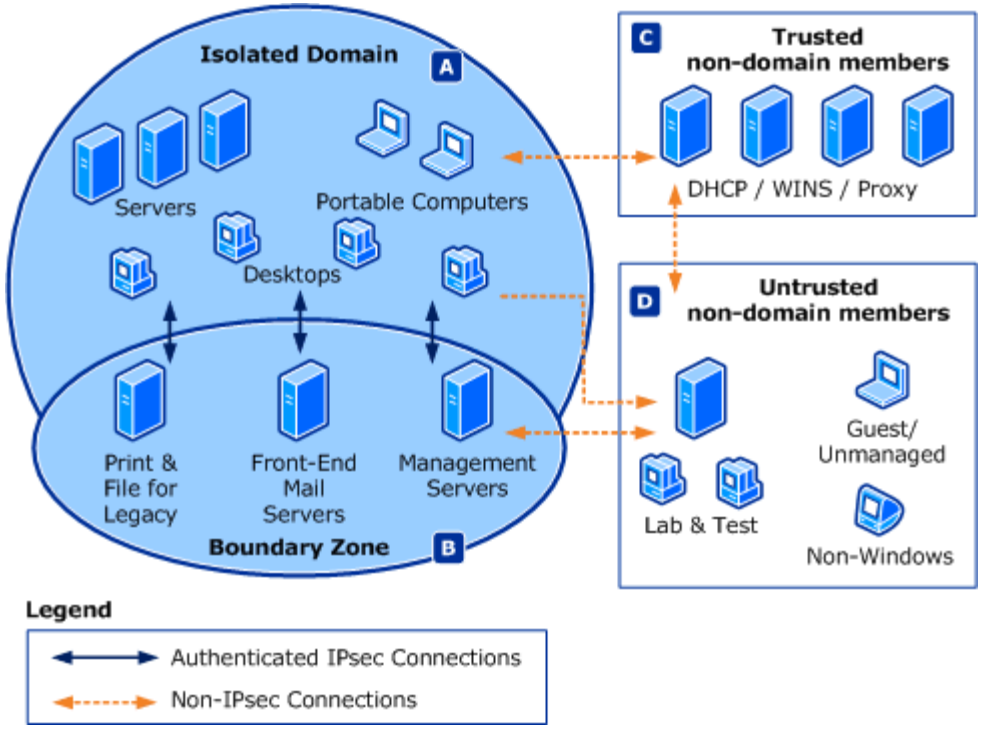
Windows Domain Isolation

Windows natively supports IPSec for domain isolation

- Blocks unauthorized non-domain access
- Authenticates all traffic
  - Mutually authenticated
- Optionally encrypts traffic

Cannot attack the invisible

- Mitigates man-in-the-middle
- Lowers service exploitation risk



Variable Trust

Access controlled by **variable trust**

- Similar to real-life credit scores

User authentication with username/password	10 points
Device authentication	10 points
Known device and location	10 points
Access to PCI database requires	**40 points**
Multifactor authentication with smart card	20 points
Access to PCI database	**GRANTED**

SANS

asiapacific@sans.org

Eric Conrad
SANS Faculty Fellow

NEW! SEC530: Defensible Security Architecture

Students will learn the fundamentals of up-to-date defencible security architecture. There will be a heavy focus on leveraging current infrastructure (and investment), including switches, routers, and firewalls. Students will learn how to reconfigure these devices to better prevent the threat landscape they face today. The course will also suggest newer technologies that will aid in building a robust security infrastructure.

October Singapore 2018

22-27 Oct | Eric Conrad

Sydney 2018

5-10 Nov | Eric Conrad