InterVision

RVA sec 2023

Network 201
A Tour Through Network Security

Rick Lull

Agenda

- Introduction – About Me
- A Quick Recap from Last Time (Network 101)
- Is Network Security Still a Thing in 2023?
- Baked In Options and Table Stakes
- Defense In Depth - Risks and Use Cases
- Recent Buzzwords and Why They May Not Matter to You
    - Or Why They Might Matter
- Questions?
- Closing

Introduction – About Me

- Currently Senior Solution Architect at InterVision
- A Varied Tech Career
  - PCs, Help Desk, Servers, Network, Network Security, Security, etc
- Third Time RVASec Speaker
- Lots of certs, if you care about that kind of thing

A 180 Second Recap of 101

Well, maybe not only 180 seconds…

Network 101 Recap

- The foundation – OSI Model
- IP Networking
- ICMP, TCP and UDP, Oh My!
- Routing and Routed Protocols
- Design and Implement appropriate network architectures

Isn’t Network Security Old and Busted?

- No.

Some Basics – The Table Stakes

- Have a plan
- Figure out what you have
- Consider the risks
- Secure your infrastructure

Defense In Depth Network Security

Defending Your Stuff – The Foundation

- Start from the data
    - Which probably means the applications
- Figure out what you have
    - Determine the business owner
- Consider the risks
- Policy/Procedure/Guidelines/Standards
- Data lifecycle

Defending Your Stuff – The Standard Layers

Protect:

- Access Controls – User onboard, offboard; Need to know/least privilege; Multifactor Auth/SSO; NAC
- Testing (pen tests, DR tests, etc)

Detect:

- Instrumentation – netflow, utilization, etc
- Logs – Actually MONITOR and ALERT

Respond:

- Have a plan and execute; adjust if necessary

Recover:

- Backups, Rebuilding, Lessons Learned

Defending Your Stuff – Self Hosted Apps

- Segmentation
- Inspect general content (IPS/IDS)
- Filtering app traffic inbound (WAF)
- Filtering user traffic outbound (DLP/Web Filtering/App Filtering)
- Cloud Security Posture Management (CSPM)

Defending Your Stuff – SaaS Apps

- Know the shared responsibility model for your app and vendor!
- Cloud Access Security Broker (CASB)
- Secure Access Service Edge (SASE)
- Zero Trust Network Access / Architecture (ZTNA)

Recent Buzzwords

InterVision

Buzzy or Busted?

Why they Matter Or Not Matter to you

Secure Access Service Edge

Zero Trust Network Access

SASE

- In General:
  - “A Cloud Based Security framework that combines networking and security functions together”

An Evolution, not a Revolution

No Matter What your Salesguy Says

ZTNA

- In General:
  - “An IT Security Solution that provides secure remote access to an organization’s applications and services, and thus, its data”

An Evolution, not a Revolution

And a difficult one to achieve, at that.

Oh.

That doesn’t sound as awesome as I thought….

Consider where your organization is going..

Remote Forever?

Return to Office NOW!

Hybrid, I guess…

Where is my data? Where will my data be?

Let’s Recap

The Recap

Network Security is
Still here
Still applicable
Still important
Not going away, anytime soon

Consider your situation, and plan

Secure the infrastructure

Secure the data

Secure the users

Don’t rest

Questions?

InterVision

Thank You.

InterVision