Break

Background:

- Luke Polson- Cybersecurity Analyst
- Been with MOREnet 3 (almost 4) years
- Before that worked in K-12 and Higher Education IT doing Network, Database, and Server Administration
- Firewalls: My home network uses the UniFi Security Gateway, I've worked on pfSense and Fortigate in the past.
- Hobbies: Farming and Overwatch
- E-mail: polsonjl@more.net

Outline:

- Differing Strategies for Securing Traffic
- The Talk
- Policies and Procedures
- Firewall Setup Configuration
- Logging
- Exercise: The good, the bad and the ugly
- Finding Known Good Traffic
- Test
- Creating Documentation
- Backing Up Configurations
- Exercise: Creating Firewall Rules for Allowed Traffic
- Moving Forward

Differing Strategies for Securing Traffic

“Standard” Configuration

- Allow All Outgoing
- Deny All Incoming
- Default Configuration out of the box
- Shuts down some malicious traffic
- Doesn’t encourage knowing what applications are being used or what traffic is passing over your network

Perimeter Based

- Known good traffic allowed
- All other traffic blocked at the firewall
- Works well for organizations that have strong controls over applications and workstation usage

Disadvantages:

- Is not a great model for orgs that have less control over traffic
- Depending on it's configuration may not control host-to-host traffic well

Host Based

- Known good traffic is allowed at the host
- All other traffic blocked at the host level
- Works better for organizations with widely varied usage
- Allows for targeted protection of valuable assets

Disadvantages:

- If hosts aren't updated, controls may be circumvented
- Local firewalls consume additional computing resources

Defense in Depth

Ideally, a combination of both perimeter and host.

- Perimeter only allows known good traffic in and out
- Hosts block unnecessary internal network communication
- VLANS segment uses, buildings, and/or types of users

With many other security controls in place….

The Talk

Charting a course

Now for a difficult conversation.

- Communicate the risk
- Analyze the organizational needs
- Find the intersection….

Policies and Procedures

Policy

Should be high level and approved by administration.

Could be part of the Acceptable Use Policy or the Network Security Policy

A way to add new applications or open up ports and IPs should be provided to users. (Within reason)

Policy should enshrine regular reviews of firewall configuration.

Procedures

Overlaps with documentation. Step-by-step details on how to perform associated tasks.

Created for many reasons but a couple are to ensure conformity and in case another administrator has to take over.

Policy Examples

From UMSL

All organization network traffic to and from the Internet must go through the firewall. Any network traffic going around the firewall must be accounted for and explicitly allowed by the Security Contact.

Changes and updates can be requested for the organization firewall. These changes must go through an approval process. Once the change is approved by the Security Contact, the requester is notified and the rule change is scheduled. If you need additional information, you can refer to the firewall policy. If you would like to submit a request, you can fill out the change request form.

Policy Examples Continued

From Orchard Farm

The IT department has an approved firewall operating at all times and properly configured.

Two more example policies with greater policy detail are included in the Resources slide.

Firewall Setup Configuration

Initial Setup

- BEFORE hooking up internet access, if possible, change default account usernames and passwords
- If possible restrict password retries and set account lock out settings
- Change the default host name
- If possible configure connection to Firewall GUI over https
- Configure idle timeout
- Connect to the internet and update firmware to newest stable release
- Make sure the time is properly synced to a NTP server
- Put the firewall in a secured location

Performance Considerations:

- If you are not using a feature, turn it off.
  - Unless you need traffic shaping, turn it off.
- Log only what you will need and are willing to regularly review
- When creating rules arrange the most used rules so they are processed by the firewall first
- When creating rules avoid using Any or 0.0.0.0
  - The more specific you can make rules, the better

Logging

Minimum Logging Recommendations:

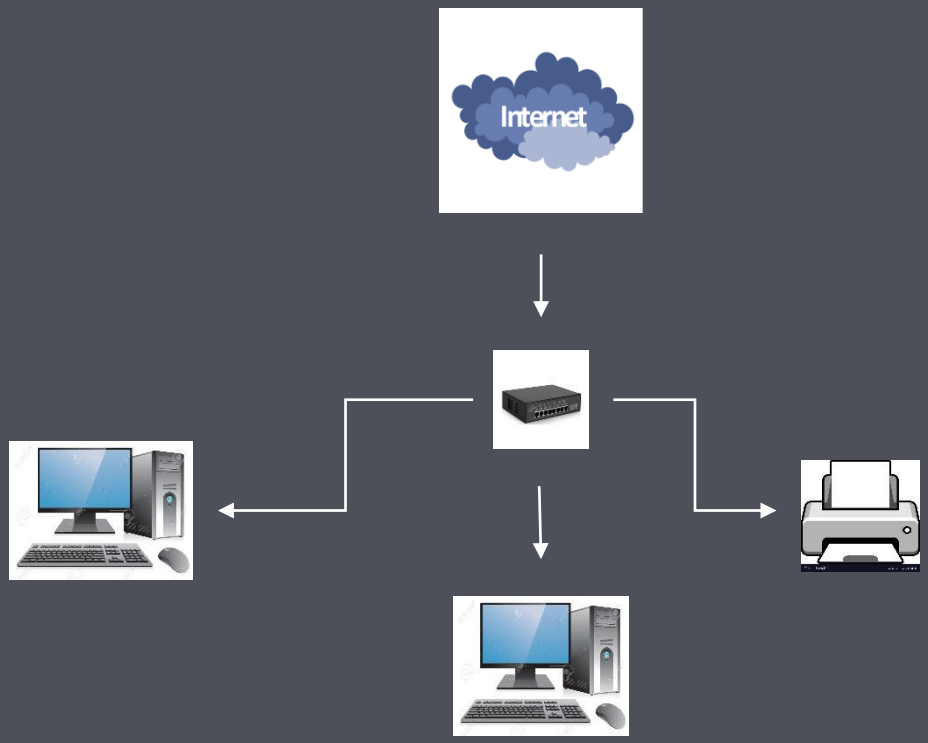
- Log outgoing connections
- Internal/External IP
- Internal/External Port
- NTP synced timestamp
- Keep a week's worth

Additional Logging Suggestions:

- Log traffic between VLANS
- Have an external log store
- Consider alerting on: rule changes/disables, reboots, high resource utilization, device logon

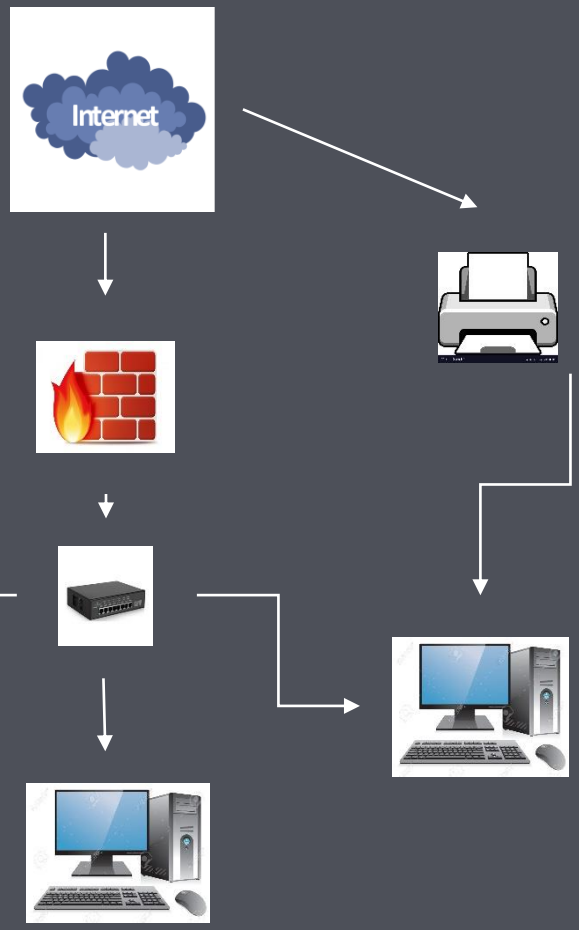
Exercise:

The Good, The Bad, and The Ugly



Be better connected.

Allow all Outgoing
Deny all Incoming
EXCEPT
Port forward from 25398 to 3389 for server RDP



Allow Outgoing
Port 80 and 443
Deny all Incoming

Guest VLAN:
Traffic
segregated
from
production
network

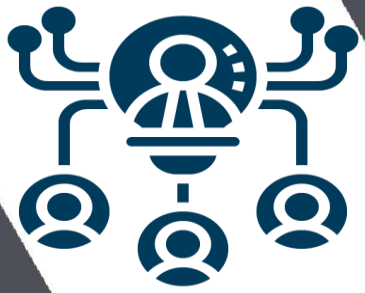
Be better connected.

Finding Known Good Traffic

Considerations for Egress Filtering

- Every application in use on the network needs to be collected before beginning
- There needs to be a approval process in place for new applications
- There will be increased administrative overhead

Resources Available



- Documentation
- Vendors
- DIY (Wireshark)

Test

Test the configuration

You DO NOT want to roll Egress filtering live without testing it first.

If you do, you and your users will have a bad week. It will also generate ill will towards IT and the policy.

If possible, create a test network and have users interact with workstations as normal, have a reporting process when things break.

Other Testing

- Make sure you can access firewall management
- Verify logging
- Do load testing, simulate a DoS see if the firewall and configuration can handle the strain
- Test additional services that have been enabled

Creating Documentation

What you should document:

- Rules and their descriptions
- Dated created for rules
- How to access (UN/PW)
- Network diagram

Backing Up Configurations

Backups are important!

- Every firewall product we are aware of has a way to backup it's configuration.
- Setting up deny-all takes time, you do not want that time wasted by a borked firmware update.
- Set a regular time to update backups.
- Store backups in a secure, offline location.
- Test the backups.
- Testing can be problematic. Before you test be sure you can take an extended outage and have adequate documentation of your configuration.
- Resource slides contain links to back up instructions for major firewall products.

Exercise:

Creating Firewall Rules for Known Good Traffic

Moving Forward:

Ongoing Firewall Management

Management Tasks:

- Keep patching and firmware up-to-date
- Monitor account access and rule changes
- Review logs and alerts
- Update rules and documentation
- Check computing resources used/capacity
- Review organizational needs and firewall deployment based on risk

Questions?

Thank you!

Resources:

NIST Guidelines on Firewalls and Firewall Policy: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=901083

Texas Wesleyan Firewall Policy: https://txwes.edu/media/twu/content-assets/documents/it/policyprocedures/firewall-policy.pdf

Northwestern University Firewall Policy: https://www.it.northwestern.edu/policies/firewall.html

Resources- Backups:

- Fortigate- https://help.fortinet.com/fos60hlp/60/Content/FortiOS/fortigate-getting-started/basic-admin/configuration-backups.htm?Highlight=backup
- SonicWall- https://www.sonicwall.com/support/knowledge-base/using-the-system-backup-feature/170503689756958/
- Cisco- https://community.cisco.com/t5/security-documents/how-to-backup-asa-configuration-through-asdm/ta-p/3155782
- Sophos- https://community.sophos.com/kb/en-us/123145
- pfSense- https://docs.netgate.com/pfsense/en/latest/backup/index.html

Resources- Configuration:

- Fortigate- Getting Started https://docs.fortinet.com/document/fortigate/6.0.0/handbook/295300/system-settings
- Fortigate- Best Practices https://docs.fortinet.com/document/fortigate/6.0.0/handbook/574517/best-practices
- SonicWall- Getting Started https://www.sonicwall.com/support/knowledge-base/sonicwall-out-of-the-box-setup/170505828413340/
- SonicWall- Best Practices https://www.sonicwall.com/support/knowledge-base/popular-sonicwall-firewall-configurations/170503358114735/

Resources- Configuration 2:

- Cisco ASA 5500-X Install Guides: https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-guides-list.html
- Cisco ASA 5500-X Configuration Guides: https://www.cisco.com/c/en/us/support/security/asa-5500-series-next-generation-firewalls/products-installation-and-configuration-guides-list.html
- Sophos XG Firewall Online Documentation: https://docs.sophos.com/nsg/sophos-firewall/18.0/Help/en-us/webhelp/onlinehelp/nsg/concepts/GettingStarted.html

Resources Configuration 3:

- pfSense Documentation: https://docs.netgate.com/pfsense/en/latest/
- Basic Windows Firewall Policy: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-firewall/planning-settings-for-a-basic-firewall-policy
- How Windows Firewall Applies Rules: https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc755191(v=ws.10)?redirectedfrom=MSDN

MOREnet

Be better connected.

(800) 509-6673
www.more.net