

Operational Security Current Practices

(draft-opsec-current-practices-03.txt)

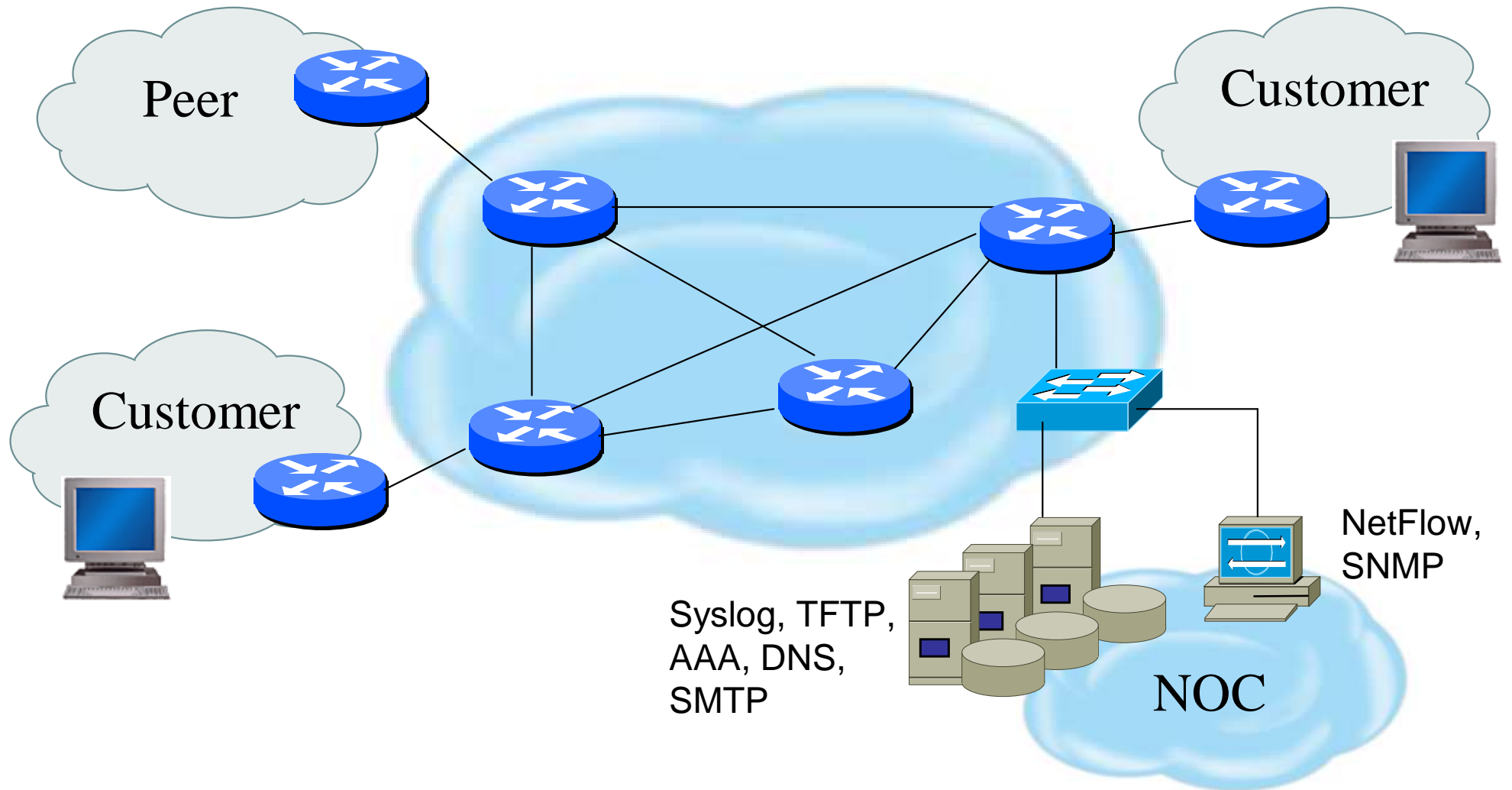
Merike Kaeo

Double Shot Security

merike@doubleshotsecurity.com



Infrastructure Security



How Are We Protected?

- Understand the Problem
- Establish an Effective Security Policy
 - physical security
 - logical security
 - control/management plane
 - routing plane
 - data plane
- Have Procedures In Place For Incident Response
 - assessing software vulnerability risk
 - auditing configuration modifications



Attack Sources

- **Passive vs Active**
 - Writing and/or reading data on the network
- **On-Path vs Off-Path**
 - How easy is it to subvert network topology?
- **Insider or Outsider**
 - What is definition of perimeter?
- **Deliberate Attack vs Unintentional Event**
 - Configuration errors and software bugs are as harmful as a deliberate malicious network attack



Operational Security Impact

- Unauthorized Disclosure
 - circumstance or event whereby entity gains access to data for which it is not authorized
- Deception
 - circumstance or event that may result in an authorized entity receiving false data and believing it to be true
- Disruption
 - circumstance or event that interrupts or prevents the correct operation of system services and functions
- Usurpation
 - circumstance or event that results in control of system services or functions by an unauthorized entity



Security Services

- User Authentication
- User Authorization
- Data Origin Authentication
- Access Control
- Data Integrity
- Data Confidentiality
- Auditing / Logging
- DoS Mitigation



Functional Considerations

- Device Physical Access
- Device In-Band Management
- Device OOB Management
- Data Path
- Routing Control Plane
- Software Upgrade / Configuration Integrity

- Logging
- Filtering
- DoS Tracking
 - Sink Hole Routing
 - Black-Hole Triggered Routing
 - Unicast Reverse Path Forwarding (uRPF)
 - Rate Limiting



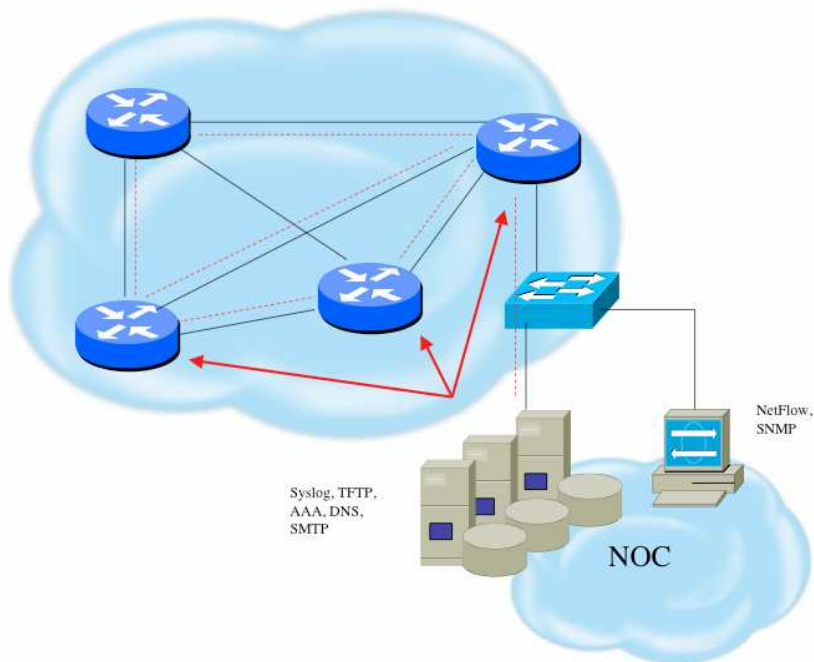
Device Physical Access

- Equipment kept in highly restrictive environments
- Console access
 - password protected
 - access via OOB management
- Individual users authenticated
- Social engineering training and awareness



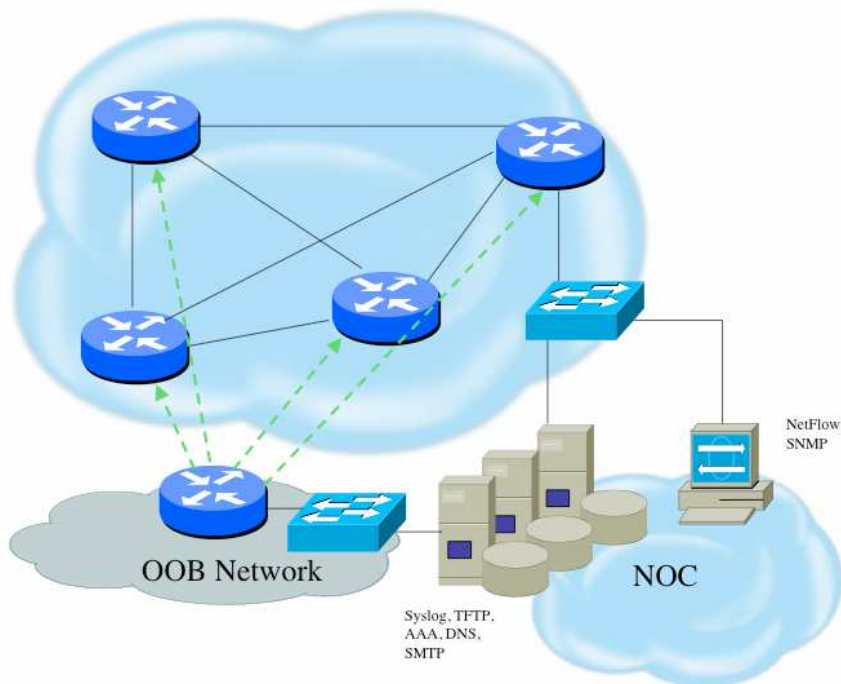
Device In-Band Management

- SSH primarily used; Telnet only from jump hosts
- All access authenticated
 - Varying password mechanisms
 - AAA usually used
 - Single local db entry for backup
- Individual authorization
- Strict access control
- Access is audited with triggered pager/email notifications
- SNMP is read-only
 - Community strings updated every 30-90 days

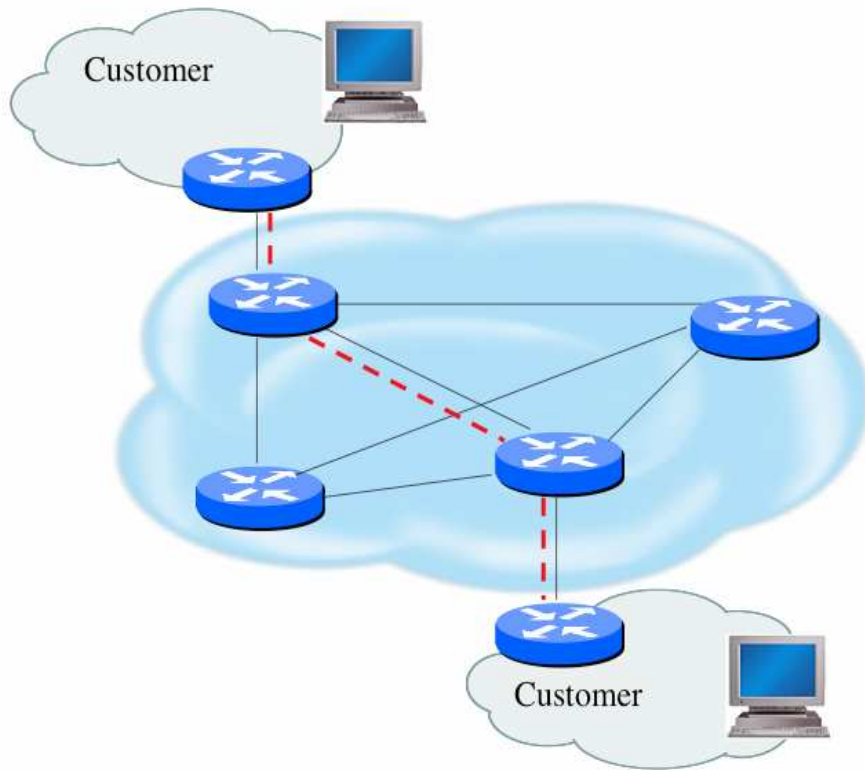


Device OOB Management

- SSH primarily used; Telnet only from jumphosts
- All access authenticated
 - Varying password mechanisms
 - AAA usually used (server typically different for in-band vs OOB)
 - Single local db entry for backup
- Individual authorization
- Strict access control
- Access is audited with triggered pager/email notifications
- SNMP is read-only
 - community strings updated every 30-90 days

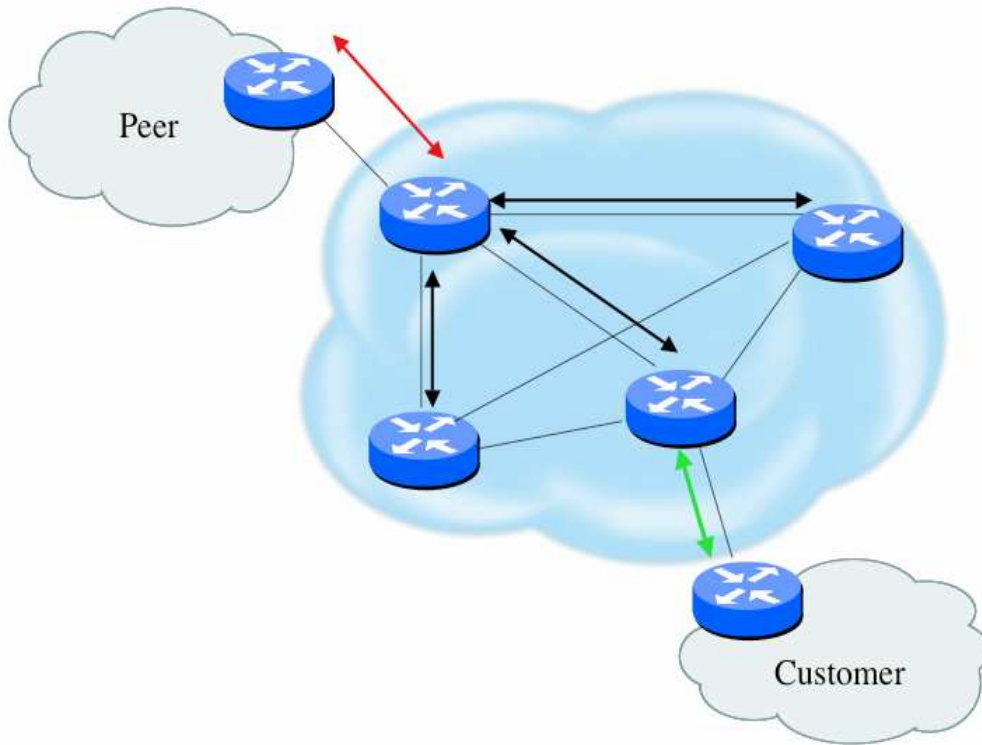


Data Path



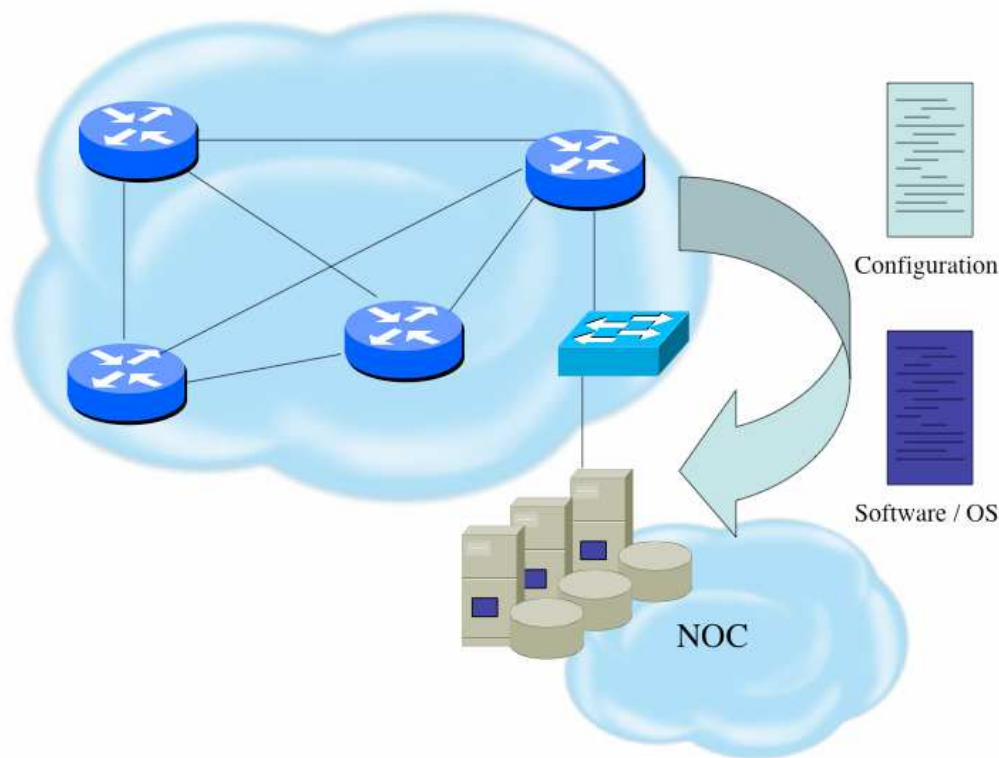
- Filtering & rate limiting are primary mitigation tools
- BCP-38 guidelines for ingress filtering
- Null-route and black-hole malicious traffic
- Netflow audits traffic flows
- uRPF is not consistently implemented
- Logging of Exceptions

Routing Control Plane



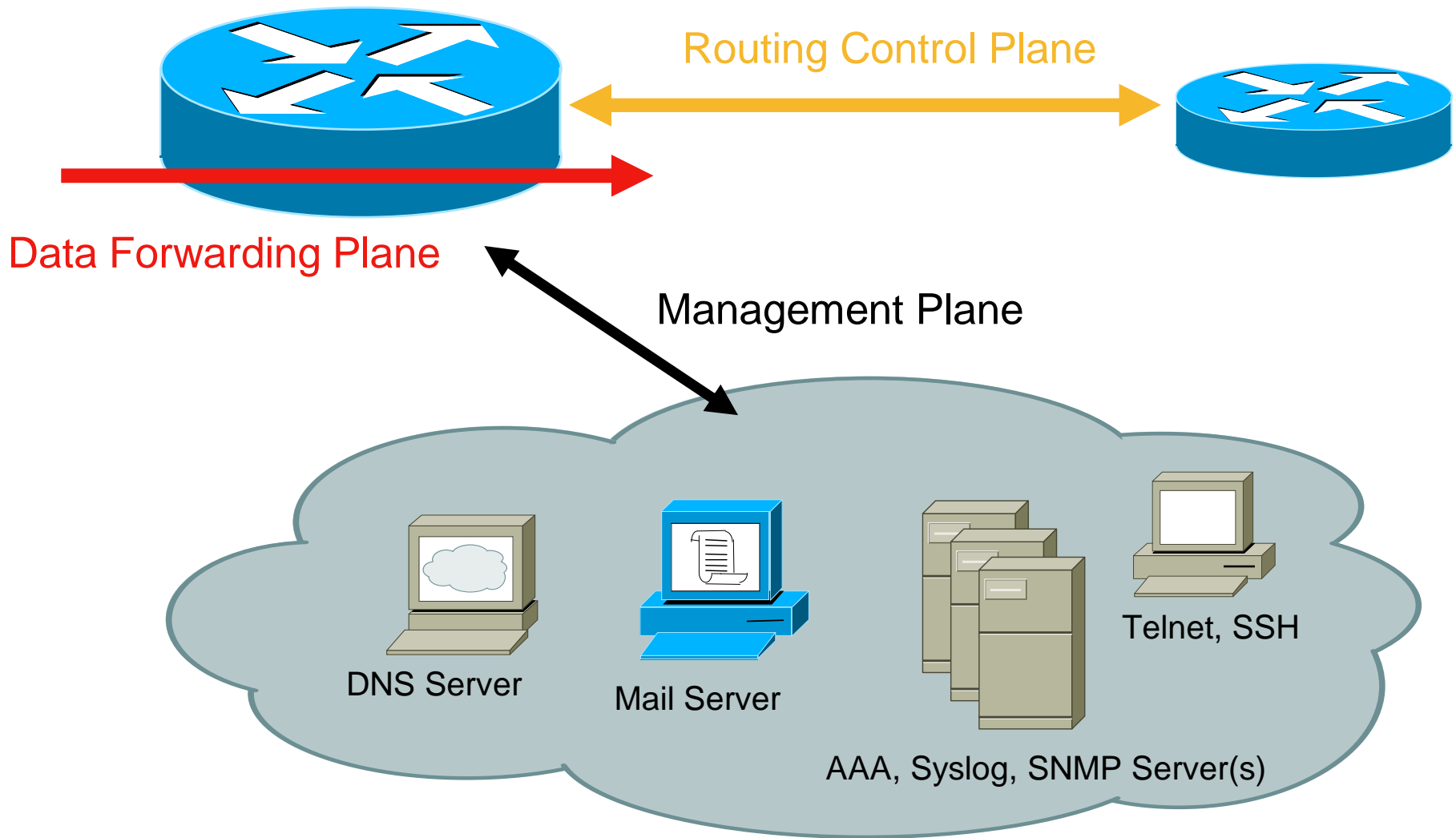
- MD-5 authentication
 - Some deploy only at customer's request
- Route filters limit what routes are believed from a valid peer
- Packet filters limit which systems can appear as a valid peer
- Limiting propagation of invalid routing information
 - Prefix filters
 - AS-PATH filters (trend is leaning towards this)
 - Route dampening (causes more harm than good)
- Not yet possible to validate whether legitimate peer has authority to send routing update

Software Upgrade / Integrity



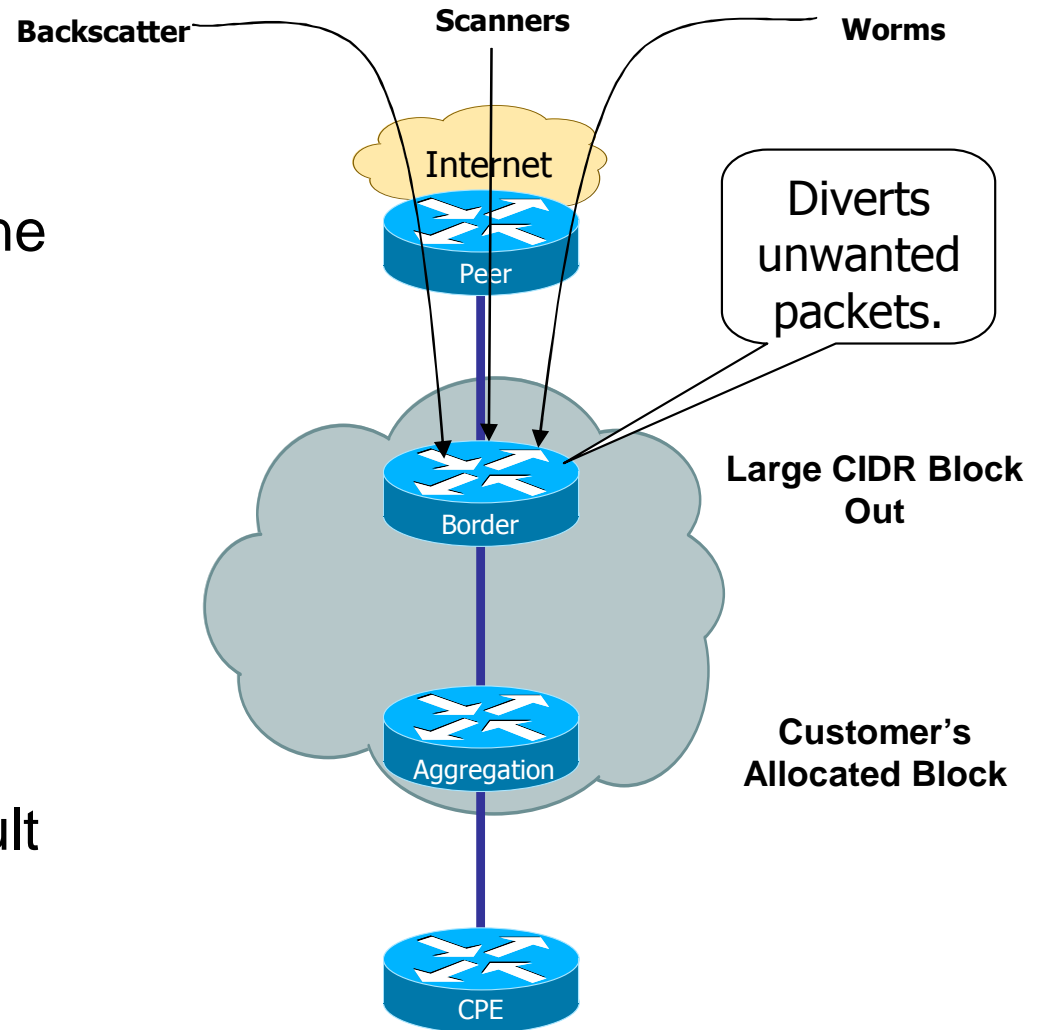
- Files stored on specific systems with limited access
- All access to these systems are authenticated and audited
- SCP is used where possible; FTP is NEVER used; TFTP still used
- Configuration files are polled and compared on an hourly basis
- Filters limit uploading / downloading of files to specific systems
- Many system binaries use MD-5 checks for integrity
- Configuration files are stored with obfuscated passwords

Filtering Considerations



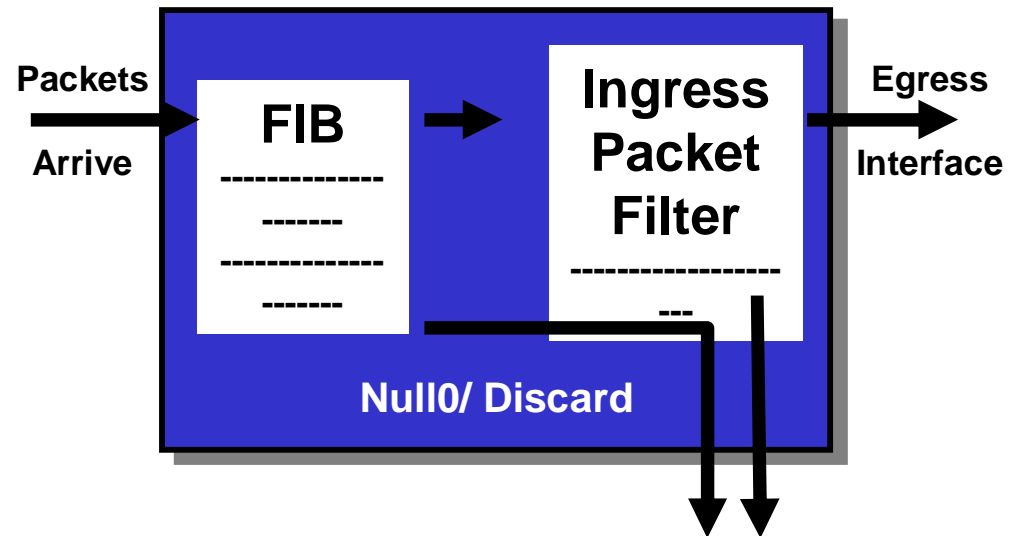
DoS Tracking / Mitigation (Sink Hole)

- Router or workstation built to *divert traffic* and assist in analyzing attacks and determine the source.
- Used to redirect attacks away from the customer by using a router built to withstand the attack.
- Used to monitor *attack noise, scans, data from mis-configuration* and other activity (via the advertisement of default or unused IP space)



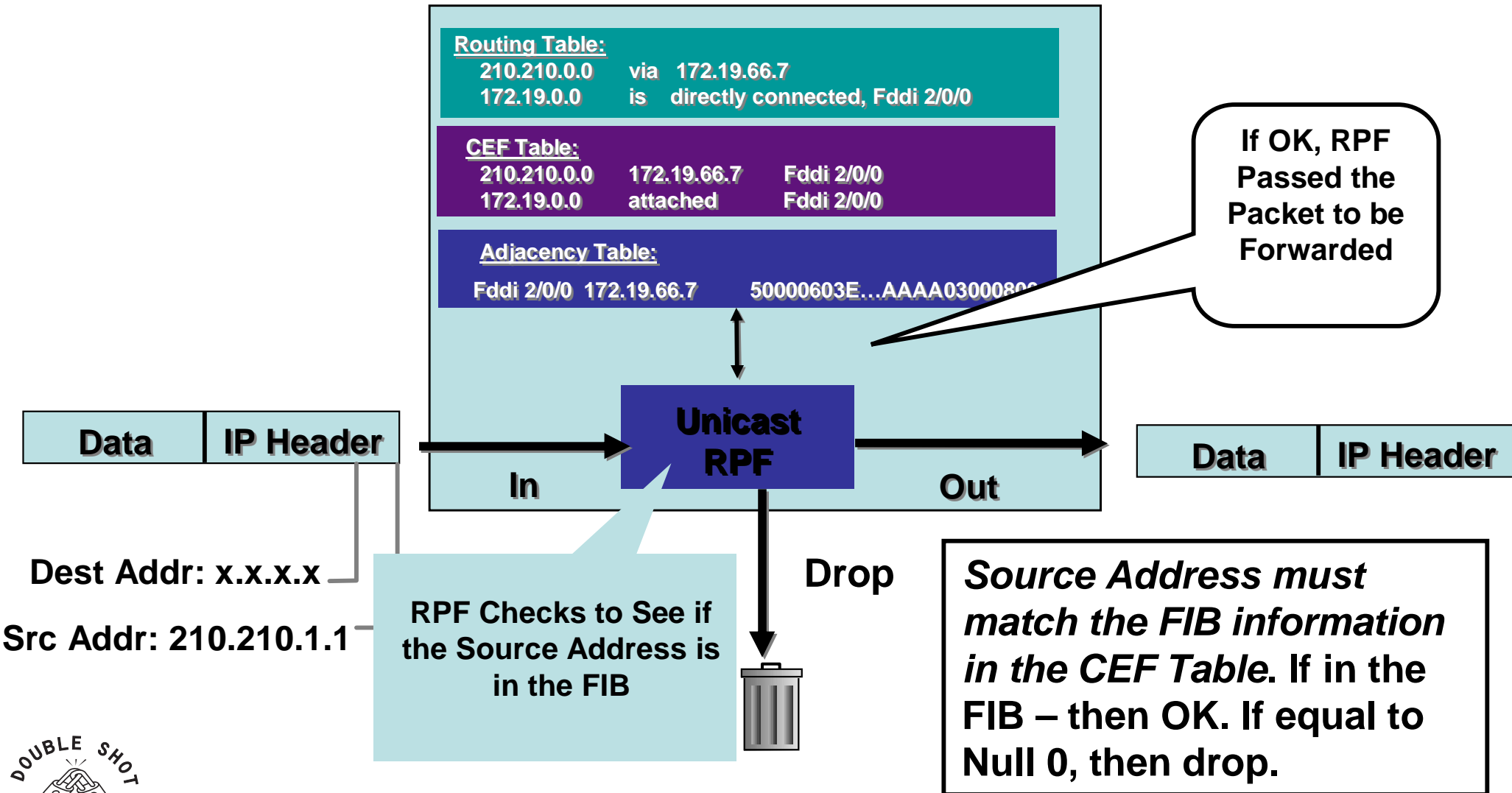
DoS Tracking / Mitigation (Black-Hole Routing)

- Several Techniques:
 - Destination-based BGP Blackhole Routing
 - Source-based BGP Blackhole Routing (coupling uRPF)
 - Customer-triggered
- Exploits router's forwarding logic which typically results in desired packets being dropped with minimal or no performance impact



- Forward packet to the Bit Bucket
- Saves on CPU and ACL processing

DoS Tracking / Mitigation (uRPF)



IPv4 vs IPv6

- Same considerations exist for IPv6 networks although the same tools are not yet there for IPv6 transports
- IPv6 / IPv4 tunnels used to hide malicious traffic from filtering rules is a concern
- Flow collection tools are not yet capable of detecting much malicious traffic



Operational Practices Summary

- Risk mitigation techniques in varying ISPs are similar yet different
 - Similar conceptual safeguards
 - Differences based on performance issues and operational complexity
- Infrastructure products need standardized capabilities for more effective security deployments



How Can You Help Finalize This Work ?

- Are there techniques you are using that are different?
- Are there requirements you need which are not listed?
- Please provide input.....

