Router Security - Approaches and Techniques You Can Use Today

Neal Ziring
System and Network Attack Center
Information Assurance Directorate
National Security Agency

Introduction and Outline

GOAL:
Define a conceptual basis for router security and give examples of specific current techniques

OUTLINE:
– Motivations
– Conceptual Structures
– General Areas and Policies
– Specific Techniques
– Currently Available Resources
Motivations

Protect your routers...
– to improve your control of your networks
– to reduce downtime due to attacks and accidents
– to hide information about your network
– to protect your customers and clients
– to protect your partners
– to protect your country

Conceptual Structures (1)

Security for routers, or any piece of network infrastructure, must be:
– driven by threat
– documented in policy
– implemented in router configurations
– maintained with consistent procedures
– audited and tested for assurance
Conceptual Structure (2)

- Threats
  - Best Practices
  - Local Policies
  - Security Controls

- Protect Network Traffic
- Protect Static Configuration
- Protect Dynamic State

Conceptual Structure (3)

- Protect Static Configuration
- Protect Dynamic State
- Protect Network Traffic

Mgmt. Plane | Control Plane | Data Plane
---|---|---
✓ | ✓ | ✓
✓ | ✓ | ✓
✓ | ✓ | ✓
Typical Policy Elements

Protect Static Configuration:
- only authorized administrators can log in to the router, and all login identities must be authenticated
- all remote administration sessions must be protected

Protect Dynamic State
- only internal monitoring stations may gather traffic stats
- routing updates should be accepted from authorized partners and interior routers only

Protect Network Traffic
- no traffic from unroutable addresses may cross the router
- ICMP may consume no more than 5% of link bandwidth

Protect Static Configuration (1)
- Requirement:
  only authorized administrators may log in to the router, only from authorized networks, and all login identities must be authenticated.
- Threats Addressed:
  login by hostile agents or unauthorized users, inability to attribute actions to accountable individuals
- Mechanisms to use:
  - Local username/password settings on router (no shared accounts!)
  - Address-based controls/filters on session services or protocols
  - Centralized username/password authentication via AAA (RADIUS or other protocols)
  - Centralized cryptographic authentication (Kerberos or SSL w/PKI)
Protect Static Configuration (2)

- **Requirement:**
  all remote administration sessions must be protected.

- **Threats addressed:**
  Exposure of sensitive information to unauthorized listeners, session hijacking.

- **Mechanisms to use:**
  - Set up and permit only encrypted remote admin protocols (e.g. SSH, Kerberized Telnet, HTTPS)
  - Set up IPSec between administrator workstations and routers
  - Perform all administration over an isolated back-end network

Protect Dynamic State (1)

- **Requirement:**
  only internal monitoring stations may gather network traffic and performance statistics.

- **Threats Addressed:**
  exposure of network architecture information, exposure of sensitive information about clients' network use

- **Mechanisms to use:**
  - Address-based filters on management protocols (SNMP, NetFlow)
  - Strong authentication and encryption on management protocol sessions (SNMPv3)
  - Gather traffic statistics over an IPSec VPN
Protect Dynamic State (2)

- **Requirement:**
  accept routing updates only from interior routers and authorized partners only.

- **Threats Addressed:**
  - malicious mis-routing, denial of service

- **Mechanisms to use:**
  - Address-based protocol-specific filters on interfaces
  - Address-based filters on routing protocols
  - Shared-secret authentication of routing updates

Protect Network Traffic (1)

- **Requirement:**
  - No traffic from unroutable or reserved addresses should traverse the router.

- **Threats Addressed:**
  - address-spoofed DDoS traffic exiting your network, forwarding bad traffic to peers

- **Mechanisms to use:**
  - interface filters for RFC1918 and IANA reserved addresses
  - Unicast RPF
  - null routing (various approaches)
Protect Network Traffic (2)

- **Requirement:**
  ICMP may consume no more than 5% of link bandwidth.

- **Threats addressed:**
  Flooding attacks or DDoS attacks using ICMP.

- **Mechanisms to use:**
  - Committed Access Rate (CAR) rate limiting
  - QoS / Traffic Policing

Some Resources

Sample Security Resources for Routers:
- Cisco Systems routers
  - *Hardening Cisco Routers*, available from O'Reilly Associates
- Juniper Networks routers
  - *CIS JunOS Router Security Benchmark* [coming soon]
- Foundry Networks routers
Summary

• Use your general security policies and router security best practices help you harden your router configuration
• Think about router security with a layered model:
  – physical integrity
  – static configuration
  – dynamic state
  – network traffic
• Today's devices have many facilities that you can use to enforce security policies
• Don't just configure security, test it!