CPU Protection Mechanisms

https://t.me/learningnets

CPU Protection Mechanisms

- Scheduler Interval
  - Guarantees CPU for low-priority processes
    - Enable with **scheduler interval** (or **scheduler allocate**)
- Logging Interval
  - Controls the amount of generated log messages
    - **logging rate-limit**
- CPU Threshold Notifications
  - Enable with **process cpu threshold type [total | process | interrupt]** [*options*]

https://t.me/learningnets

Memory Protection Mechanisms

https://t.me/learningnets

Memory Protection Mechanisms

- Memory Reservation
  - Increase the default console memory (256KB) with **memory reserved console**
    - Use **dir nvram:** to find an optimal value
    - Check with **show memory console reserved**
  - Use **memory reserve critical** to allocate memory for critical notifications
- DRAM Allocation
  - Control the amount of I/O Memory with **memory-size iomem**
- Memory Threshold Notifications
  - Enable with **memory free low-watermark [processor | io]**

https://t.me/learningnets

Management Plane Protection

https://t.me/learningnets

Management Plane Protection (MPP)

- Simplifies device access control on IOS
  - Restricts management traffic to the management port(s) only
    - Other interfaces drop to-the-box management traffic
      - Transit management packets are not affected
  - Dropped packets don't affect CPU
  - Works for BEEP, FTP, HTTP, HTTPS, Telnet, TFTP, SSH, and SNMP

https://t.me/learningnets

MPP Configuration

- Activated through the CPPr syntax

  control-plane host

  management-interface *interface* **allow** *[protocol]*

- Verification
  - **show management-interface**

https://t.me/learningnets

IP Spoofing Attacks

https://t.me/learningnets

IP Spoofing Overview

- A process of crafting packets with false source IP addresses
  - Identity Hiding
    - Random value
  - Impersonation
    - Existing address
- Often combined with other attacks
  - DoS, Flooding, MiTM, etc.

https://t.me/learningnets

IP Spoofing Mitigation

- Early blocking
  - E.g. Network Edge
  - Access-Lists and/or uRPF

https://t.me/learningnets

IP Spoofing Mitigation

- IPv4/IPv6 ACL Guidelines
  - RFC 1918
  - RFC 2827 (BCP 38)
    - Updated by RFC 3704 (BCP 84)
    - Ingress/Egress Filtering of illegitimate addresses
  - RFC 6890 (BCP 153)
    - Special IPv4/IPv6 addresses („Martians")
      - 0.0.0.0/8, 127.0.0.0/8, fe80::/10, ::/128 and more
  - Unallocated addresses

https://t.me/learningnets

DoS Attacks

https://t.me/learningnets

Denial of Service (DoS) Overview

- Any offensive activity performed to render a system unusable
  - Not a single attack
  - DoS vs Distributed DoS (DDoS)
    - Zombies/Bots and Botnets

- DoS/DDoS Attack Types
  - Flooding
    - ICMP Echo (Smurf), UDP Echo (Fraggle), TCP SYN, etc.
  - Control Plane
  - State Disruption and more

https://t.me/learningnets

DoS/DDoS Mitigation

- Flooding
  - Blocking
    - Firewalls, IPv4/IPv6 ACLs, static uRPF, shunning, etc.
  - Rate Limiting
    - QoS Policing
  - TCP Intercept and Inspection
  - Remotely Triggered Black Hole Filtering (RTBH)

https://t.me/learningnets

DoS/DDoS Mitigation

- Control Plane
  - CPU Protection Mechanisms
    - CoPP
    - CPPr
  - Routing Protocol Authentication
  - L2/L3 protocol-specific features

- State Disruption
  - Authentication
  - Application/OS Hardening and more

https://t.me/learningnets

TCP Intercept

https://t.me/learningnets

TCP Intercept Overview

- IOS TCP Syn Flood mitigation tool
  - IPv4

- Modes of Operation
  - Intercept
    - Router as a Proxy
  - Watch
    - Session monitoring

https://t.me/learningnets

TCP Intercept Operations

- Attack detection is based on configurable thresholds
  - One-Minute
    - Connection request rate
    - **ip tcp intercept one-minute [low | high]** *threshold*
  - Incomplete
    - Half-open connections
    - **ip tcp intercept max-incomplete [low | high]** *threshold*

- Exceeding one of the tresholds enables Aggressive Mode
  - Aggressive behavior stops when both „low" thresholds are met

https://t.me/learningnets

TCP Intercept Operations

- Aggressive Mode
  - Each new connection attempt triggers a removal of one half-open session
    - **ip tcp intercept drop-mode [oldest | random]**
  - Certain timers are halved
    - TCP retransmission
      - Intercept Mode
    - Watch Timer
      - Watch Mode
      - **ip tcp intercept watch-timeout**

https://t.me/learningnets

TCP Intercept Configuration

- Designate traffic for inspection
  - **ip tcp intercept-list** *acl*
    - The source is usually set to „any”
- Select Inspection Mode
  - **ip tcp intercept mode [intercept|watch]**
- Define the attack thresholds
  - **ip tcp intercept one-minute [low | high]** *threshold*
  - **ip tcp intercept max-incomplete [low | high]** *threshold*

https://t.me/learningnets

Remotely Triggered Black Hole Filtering

https://t.me/learningnets

Remotely Triggered Black Hole (RTBH) Filtering

- Routing-based traffic filtering method
  - Widely adopted by many ISPs to mitigate (D)DoS or worm attacks
- RTBHs are controlled by BGP
  - Requires iBGP peerings between the triggering device and edge routers
    - Black hole activation happens through a special static route
- Works equally well for IPv4 and IPv6

https://t.me/learningnets

RTBH Variants

- Destination-Based
  - Trigger advertisement includes the target host/network
    - Blocks all traffic sent to the victim
- Source-Based
  - Trigger advertisement includes the attacker's address(es)
    - Usually hard to implement
  - Requires uRPF

https://t.me/learningnets

RTBH Filtering Configuration

- iBGP Peerings
  - Trigger – Edge
    - If using Route Reflection, peer with the RR Server
    - **neighbor remote-as**
  - BGP Community exchange
    - **neighbor send-community**

- All BGP speakers
  - Non-existing host route to Null0
    - **ip route** *BH-IP* **255.255.255.255 null0**
    - **ipv6 route** *BH-IP* **/128 null0**

https://t.me/learningnets

RTBH Filtering Configuration

- Triggering Device

```
route-map rname permit 10
  match tag tag
  set local-preference high_value
  set community no-export
  set [ip|ipv6] next-hop BH-IP

router bgp asn
  redistribute static route-map rname

[ip | ipv6] route src/dst BH-IP tag tag
```

https://t.me/learningnets

RTBH Filtering Configuration

- Edge Routers
  - Silent mode
    - **no ip icmp unreachables**
    - **no ipv6 unreachables**
  - Source-Based RTBH
    - **[ip | ipv6] verify unicast source reachable-via any**

https://t.me/learningnets

IPv4 Options & Security

https://t.me/learningnets

IP Options Overview

- Created to extend IPv4 (RFC 791)
  - Part of an IPv4 Header
    - Up to 40B long
  - General Format
    - „Option Type – Data" or „Option Type – Length – Data"
  - Option Type
    - Copied Flag
      - Copy to fragments?
    - Option Class
    - Option Number

https://t.me/learningnets

IP Options Processing

- Affected by few factors
  - Device Architecture
    - General Purpose CPU only (older devices)
    - ASIC
  - Implementation
    - Forward as regular packets, ignore some & forward, process all & forward
  - Configuration
    - Granularity
- General Purpose CPU processing = high security risk

https://t.me/learningnets

IP Options Examples

- Loose Source & Record Route (LSRR) - Type 131
  - IP hops to go through to reach the destination
  - Threats
    - Firewall bypass
    - Reaching unintended systems
    - Topology mapping and more
- Strict Source & Record Route (SSRR) - Type 137
  - Exact IP path to take to reach the destination
  - Threats like with LSRR

https://t.me/learningnets

IP Options Examples

- Internet Timestamp - Type 68
  - Time recording
  - Threats
    - OS fingerprinting
    - Topology mapping
- Router Alert - Type 148
  - Used by certain applications, e.g. RSVP
  - Threats
    - CPU DoS

https://t.me/learningnets

More Examples

- RFC 7126
  - „Recommendations on Filtering of IPv4 Packets Containing IPv4 Options”

https://t.me/learningnets

IPv4 Options Attack Mitigation

https://t.me/learningnets

Mitigating IPv4 Options Attacks - IOS

- IP Options Selective Drop
  - **ip options [drop | ignore]**
- Access-Lists
  - The **option** keyword
- Control Plane Policing & Protection

https://t.me/learningnets

Mitigating IPv4 Options Attacks - ASA

- MPF
  - The default policy allows packets with Router Alert option set
    - Packets containing other options are dropped

```
policy-map type inspect ip-options _default_ip_options_map
 parameters
  router-alert action allow
```

https://t.me/learningnets

IPv4 Fragmentation

https://t.me/learningnets

Fragmentation Overview

- A process of splitting an IP packet into smaller pieces
  - A given physical network cannot forward packets larger than its MTU
    - E.g. 1500B for Ethernet
    - Lower values may be seen according to IPv4 spec (68B)
  - Outbound process

- IPv4 Fragmentation can be performed by any device
  - Highly undesirable
    - Overhead
    - Delay
    - CPU and memory for Reassembly

https://t.me/learningnets

The Process

- Uses Identification, Flags & Fragment Offset IP header fields
  - Identification
    - Distinguishes between the packets being fragmented
  - Flags
    - More Fragment
    - Don't Fragment (DF)
  - Fragment Offset
    - Offset of a fragment in the packet
      - First fragment has an offset of 0

https://t.me/learningnets

Path MTU Discovery (PMTUD)

- A dynamic method of discovering the lowest MTU of a path
  - Enabled on most OSes by default
    - Works for TCP and UDP
  - Relies on the DF bit
    - Packets with the DF bit enabled cannot be fragmented and are dropped
      - ICMP „Fragmentation needed and DF set" (Type 3, Code 4) is returned to the Sender along with the supported MTU value

https://t.me/learningnets

IPv4 Fragmentation Attacks & Mitigation

https://t.me/learningnets

Fragmentation Attacks

- Commonly used for Reconnaissance and IPS/Firewall evasion
  - If successful may open doors to other attacks
- Efficient mainly against stateless platforms & technologies
  - Buffer Overflow
    - Flooding with fragments
  - Tiny Fragment
    - Hiding Upper Layer information in non-initial fragment
  - Overlapping Fragments
    - Setting incorrect fragment offsets

https://t.me/learningnets

Mitigation Techniques - IOS

- Access-List
  - Use **fragment** to block all non-initial fragments
    - Does not affect the initial fragment and non-fragmented packets

- Virtual Fragment Reassembly (VFR)
  - Turns a router into a stateful firewall for IP fragments
  - Enable with **ip [virtual-reassembly | ip virtual-reassembly-out]** *[options]*
    - **max-reassemblies**
    - **max-fragments**
    - **timeout**
    - **drop-fragment**

https://t.me/learningnets

Mitigation Techniques - ASA

- Fragmentation protection is enabled by default
  - Works similar to VFR
  - Tune with **fragment reassembly [virtual | full]** *[options]*
    - **chain**
      - When set to 1 means drop all fragments
    - **size**
    - **timeout**

https://t.me/learningnets

NBAR & NBAR2

https://t.me/learningnets

Network-Based Application Recognition (NBAR)

- Application-level IOS traffic classification mechanism
  - Typically used along with QoS
  - Sometimes deployed to drop or rate-limit offending packets
    - E.g. HTTP worms
  - Configured with **match protocol** in a class-map
    - Requires CEF
    - Does not work for IPv6

https://t.me/learningnets

NBAR2

- Re-architectured version of NBAR available on ISR-G2 routers
  - Advanced classification
    - Full IPv6 support
    - Skype, Tor, Facetime and more
  - Attribute-based configuration
    - **match protocol attribute**
  - Easy to maintain
    - Protocol Packs (**ip nbar protocol-pack**) extend supported applications

https://t.me/learningnets

NBAR2 Attributes

- NBAR2 groups applications based on different Attributes
  - Application Group
    - Suit/brand
  - Category
    - Function
  - Sub-Category
    - Sub-function
  - P2P
  - Tunnel
  - Encrypted

https://t.me/learningnets

NBAR2 Configuration

- Specify an attribute and optionally application name
  - **match protocol attribute application-group** *group-name [app-name]*
  - **match protocol attribute category** *category-name [app-name]*
  - **match protocol attribute sub-category** *sub-category-name [app-name]*
  - **match protocol attribute p2p-technology** *[options]*
  - **match protocol attribute tunnel** *[options]*
  - **match protocol attribute encrypted** *[options]*

- Check assigned attributes
  - **show ip nbar protocol-attribute**

https://t.me/learningnets

NBAR Protocol Discovery

- Traffic detection tool similar to IP Accounting
  - Provides application names and statistics
    - Useful to build/tune QoS policies
  - Enable with **ip nbar protocol-discovery [ipv4 | ipv6]**
    - The results are displayed with **show ip nbar protocol-discovery**

https://t.me/learningnets

Extension Headers Attacks & Mitigation

https://t.me/learningnets

Extension Headers - Known Attacks

- DoS/DDoS
  - CPU processing = high security risk
    - Hop-by-Hop & Destination Options
    - Routing
    - Possibly other Extensions
- Other
  - Firewall/IPS Evasion
  - OS Fingerprinting
    - Extensions order and duplication
  - Covert Channels

https://t.me/learningnets

Mitigation Techniques - IOS

- Disabling Source Routing
  - RFC 5095 „ Depracation of Type 0 Routing Headers”
    - **no ipv6 source-route**
- Access-Lists
  - Extension Header filtering
    - **hbh**, **routing**, **routing-type** and more
- Control Plane Policing

https://t.me/learningnets

Mitigation Techniques - ASA

- MPF
  - IPv6 inspection engine is by default disabled
    - Enable with **inspect ipv6**

```
policy-map type inspect ipv6 _default_ipv6_map
 parameters
  verify-header type
  verify-header order
 match header routing-type range 0 255
  drop log
```

https://t.me/learningnets

IPv6 Fragmentation Attacks & Mitigation

https://t.me/learningnets

IPv6 Fragmentation Attacks

- Same as in IPv4
  - Used mainly for Reconnaissance and IPS/Firewall evasion
  - Common attacks
    - Buffer Overflow
    - Tiny Fragment
    - Overlapping Fragments

https://t.me/learningnets

Mitigation Techniques - IOS

- IPv6 Access-List
  - Use **fragment** to block all non-initial fragments
    - Does not affect the initial fragment and non-fragmented packets
- Virtual Fragment Reassembly (VFR)
  - Turns a router into a stateful firewall for IP fragments
  - Enable with **ipv6 virtual-reassembly [in | out]** *[options]*
    - **max-reassemblies**
    - **max-fragments**
    - **timeout**
    - **drop-fragment**

https://t.me/learningnets

Mitigation Techniques - ASA

- Fragmentation protection is enabled by default
  - Works similar to VFR
  - Tune with **fragment reassembly [virtual | full]** *[options]*
    - **chain**
      - When set to 1 means drop all fragments
    - **size**
    - **timeout**

- MPF
  - IPv6 inspection engine may drop packets with Fragment Extensions

https://t.me/learningnets

SEND Introduction

https://t.me/learningnets

Secure Neighbor Discovery (SEND) Overview

- Cryptographic method of securing IPv6 Neighbor Discovery
  - Not a new protocol
  - Defined in RFC 3971

- A need for SEND
  - Setting the Hop Limit to 255 (RFC 4861) in ND packets does not stop local attacks
    - ND Cache Poisoning
    - RA Spoofing
    - DAD DoS
    - Reply Attacks

https://t.me/learningnets

SEND Deployments

- Host – Node
  - Prevents from stealing/spoofing existing IPv6 addresses
  - Relies on Asymmetric Key Cryptography
    - Public Key Infrastructure (PKI) is not needed

- Router – Host
  - Authenticates Router Advertisements
    - Digital Certificates
  - Introduces two new ICMPv6 messages
    - Certificate Path Solicitation (Type 148, Code 0)
    - Certificate Path Advertisement (Type 149, Code 0)

https://t.me/learningnets

SEND Limitations

- SEND does not protect against all L2/L3 IPv6 threats
  - ND traffic goes in clear
  - Hosts are not authenticated
  - Certain attacks can still succeed
    - Sniffing
    - MAC Spoofing and more
  - Hard to deploy

https://t.me/learningnets

SEND Operations

https://t.me/learningnets

SEND Addresses

- SEND-protected IPv6 addresses are not arbitrary
  - Interface ID is computed cryptographically
    - Along with a Prefix makes a Cryptographically Generated Adress (CGA)

- CGA Interface ID Computation
  - Made of the last 64 bits of a SHA-1 hash
  - Function parameters
    - RSA Public Key
    - Prefix
    - Modifier & Collision Count

https://t.me/learningnets

SEND Extensions

- A CGA can be spoofed like any other address
  - SEND extends a normal ND message with several new fields
    - CGA parameters
      - RSA Public Key
      - Prefix
      - Modifier & Collision Count
    - Nonce & Timestamp
      - Replay protection
    - Signature
      - RSA Private-Key encrypted hash of the message

https://t.me/learningnets

SEND Address Verification

- Two-step process
  - Signature validation
    - Verifies message integrity and the ownership of the Private Key
  - CGA re-computation
    - Does not allow for RSA Key replacement
- Successful verification ensures the L3-L2 binding is legitimate

https://t.me/learningnets

SEND Authentication

- Router – Host deployments

- Based on Digital Certificates
  - Certificate Validation
    - Signature
      - Common PKI
    - Expiration Dates
    - Optional Revocation
  - Asymmetric Key Authentication

https://t.me/learningnets

SEND Configuration

https://t.me/learningnets

SEND Configuration Prerequisites

- Time Synchronization is critical
  - NTP
- Public Key Infrastructure
  - Router – Host
- Asymmetric Key Pair (RSA)
  - **crypto key generate rsa label** *keyname*
  - **ipv6 cga modifier rsakeypair** *kname* **sec-level** *number*

https://t.me/learningnets

SEND Host Mode Configuration

- Activate RSA Keys for CGA and generate CGAs under an interface
  - **ipv6 cga rsakeypair** *kname*
  - **ipv6 address** *address* **[link-local] cga**

- Optionally force the device to reject all non-SEND messages
  - **ipv6 nd secured full-secure**
  - Affects all relevant ND packets

https://t.me/learningnets

SEND Router Mode Configuration

- Routers
  - Identity Certificate
    - **crypto pki trustpoint** *tname*
      - **enrollment url**
      - **rsakeypair** *kname*
    - **crypto pki authenticate/enroll** *tname*
  - SEND trustpoint activation and CGAs
    - **ipv6 nd secured trustpoint** *tname*
    - **ipv6 cga rsakeypair** *kname*
    - **ipv6 address** *address* **[link-local] cga**
    - **ipv6 nd secured full-secure**

https://t.me/learningnets

SEND Router Mode Configuration

- Hosts
  - PKI membership
    - **crypto pki trustpoint** *tname*
      - **enrollment url**
    - **crypto pki authenticate** *tname*
  - SEND trustpoint activation and CGAs
    - **ipv6 nd secured trustanchor** *tname*
    - **ipv6 cga rsakeypair** *kname*
    - **ipv6 address** *address* **[link-local] cga**
    - **ipv6 nd secured full-secure**

https://t.me/learningnets

IOS CA Considerations

- IOS CA for SEND requires an additional extension
  - **crypto pki trustpoint** *tname*
    - **ip-extension unicast prefix** *prefix*
  - **crypto pki server** *tname*

https://t.me/learningnets

Wireless Basics

https://t.me/learningnets

Wireless Networking Overview

- Wireless communication uses radio waves
  - Defined in a group of 802.11 standards
  - Always half-duplex
    - Carrier Sense Multiple Access w/ Collision Avoidance (CSMA/CA)
  - Service Set Identifier (SSID) uniquely identifies a wireless network (WLAN)
  - Ad-Hoc vs Basic/Extended Service Set
    - Client-Client vs Client-Access Point (AP)
  - Successful communication requires clients to associate with an AP
    - Association can be maintained between the APs if roaming is on

https://t.me/learningnets

Wireless Architectures

- Autonomous
  - Access Points (APs) are managed individually
- Cisco Unified Wireless Network (CUWN)
  - Requires a Wireless LAN Controller (WLC) and optional management application
    - Access Point functions & configuration become centralized
      - Thus „lightweight" APs (LAPs)

https://t.me/learningnets

CUWN Basics

- WLC Discovery (simplified)
  - IP address configuration
    - DHCP or static
  - Broadcast Discovery Request
  - Previously known WLCs
  - DHCP
  - DNS

- CAPWAP secures WLC-AP communication
  - Control And Provisioning of Wireless Access Points

https://t.me/learningnets

WLC Modes & CAPWAP Basics

- WLC operates in a Local or Flex Connect (HREAP) mode
  - Local mode requires all traffic to pass through the WLC
    - Two CAPWAP tunnels
      - Control (UDP port 5247)
      - Data (UDP port 5246)
  - Flex Connect mode allows the traffic to be switched locally
    - No need for the Data tunnel
- CAPWAP Control communication is DTLS-protected

https://t.me/learningnets

Wireless Security Overview

https://t.me/learningnets

Wireless Basic Security Options

- Layer 1
  - SSID Cloaking
- Layer 2
  - MAC Filtering
  - Authentication & Key Management
    - 802.1x
  - Encryption & Integrity
    - WEP
    - WPA & WPA2
      - Personal (PSK)
      - Enterprise (802.1x)

https://t.me/learningnets

Wireless Basic Security Options

- Layer 3
  - IPsec
  - Web Authentication

https://t.me/learningnets

Wireless Advanced Security Options

- Client Exclusions
  - Blocking access under certain conditions
    - E.g. authentication or association failures
- Access-Lists
  - Per-entry direction
- AAA Override
  - Identity Networking with RADIUS

https://t.me/learningnets

Wireless Advanced Security Options

- Management Frame Protection
  - Secures management traffic
- Rogue Management
  - Detects, classifies and possibly contains Rogue APs
- Cisco IDS/IPS (CIDS/CIPS)
  - IDS Sensors (w/ legacy Cisco IPS)
  - IDS Signatures

https://t.me/learningnets

Device Hardening
ASA

https://t.me/learningnets

Device Hardening

- A process securing network elements according to best practices
  - Administrative Access
  - Management Services
    - Configuration, deactivation
  - Control Plane
  - Special Features
    - Platform/technology -specific

https://t.me/learningnets

Administrative Access

- In-band vs Out-Of-Band (OOB)
  - **management-only**

- AAA
  - **aaa-server** *server*
  - **aaa authentication [serial | ssh | http | enable] console** *server* **LOCAL**
    - **username privilege 15** and **password-policy**
  - **aaa authorization exec authentication-server**
  - **aaa authorization command** *server* **LOCAL**
  - **aaa accounting**

https://t.me/learningnets

Administrative Access

- SSH
  - **domain-name**, **crypto key generate rsa**, **ssh timeout**
  - Restrict access (**ssh**)
- HTTPS
  - **domain-name**, **crypto key generate rsa**, **http server enable, http timeout**
  - Restrict access (**http**)
- Legal Banner
  - **banner motd**

https://t.me/learningnets

Management Services

- NTP
  - **ntp authentication-key**
  - **ntp authenticate**
  - **ntp trusted-key**
  - **ntp server**

- Logging
  - **logging host**
  - **logging trap**
  - **logging enable**

https://t.me/learningnets

Management Services

- SNMPv3
  - **snmp-server group**
  - **snmp-server user**
  - **snmp-server host**

https://t.me/learningnets

Control Plane

- ASA blocks to-the-box traffic by default
  - Except for local ICMP and possibly HTTPS
- Routing Protocols
  - Authentication
    - Protocol-specific
      - Secure methods – MD5, SHA, etc.
  - Route Filtering
  - Adjacency Logging

https://t.me/learningnets

Device Hardening
IOS

https://t.me/learningnets

Administrative Access

- Terminal Lines
  - Disable unused lines (**no exec**)
  - Limit access method (**transport input**)
  - Restrict access (**ip access-group**)
  - Disconnect hung sessions (**service tcp-keepalives-in**)
  - Configure session timeout (**exec-timeout**)
  - Enable AAA (**login authentication**, **exec authorization**, etc.)
    - Define default/custom method lists with local fallback
      - **aaa authentication ... local**
      - **aaa authorization ... local**
      - **aaa accounting**

https://t.me/learningnets

Administrative Access

- SSH
  - **ip domain-name**, **crypto key generate**
  - **ip ssh [version | time-out | authentication-retries]**
- HTTPS
  - **no ip http server**, **ip http secure-server**
  - **ip http authentication aaa**
  - **ip http access-class**
- Configure Management Plane Protection

https://t.me/learningnets

Administrative Access

- Local Accounts & Password Protection
  - Password encryption (**username secret**, **enable secret**)
  - Password policy (**security password min-length**)
  - Login control (**login block-for**, **login delay**)
  - Legal notifications (**banner**)

https://t.me/learningnets

Management Services

- NTP
  - **ntp server**, **ntp authentication-key**, **ntp trusted-key, ntp authenticate**
- SNMPv3
  - **snmp-server group**, **snmp-server user**, **snmp-server host**
  - Optionally define views to limit MIB access

    snmp-server view myview internet included

    snmp-server view myview ipRouteTable excluded

https://t.me/learningnets

Management Services

- Logging
  - **service timestamps [debug | log]**
  - **logging host**
  - **logging trap**
  - **logging buffered**
- Unnecessary Services should be disabled

https://t.me/learningnets

Control Plane

- Infrastructure Access-Lists
  - Permit all authorized traffic (to-the-box)
    - E.g. routing protocols, management
  - Block possibly harmful packets (to-the-box)
    - Fragments
    - IP Options
    - Low TTL
  - Allow everything else (transit)

https://t.me/learningnets

Control Plane

- Control Plane Policing/Protection
  - **control-plane [host | transit | cef-exception]**
- Routing Protocols
  - Authentication
    - Protocol-specific
      - Secure methods – MD5, SHA, etc.
  - Route Filtering
  - Adjacency Logging

https://t.me/learningnets

Switch Hardening

- Catalyst-specific features
  - Data Plane
    - VLAN & Port ACLs
    - IP Source Guard
    - Storm Control
  - Control Plane
    - Port Security
    - Dynamic ARP Inspection

- Additional Information
  - Cisco Guide to Harden Cisco IOS Devices

https://t.me/learningnets

Cisco SAFE Overview

https://t.me/learningnets

IPv6 NAT Options

- IPv6 Network Prefix Translation (NPTv6)
  - Stateless one-to-one L3 address translation mechanism for IPv6
    - Does not change Upper Layer information
  - Designed to provide address independence
  - Available on ASR1k/CSR1k/ISR4k
    - Configured with **nat66 [inside|outside|prefix]**

- NAT64
  - IPv6 transition mechanism

https://t.me/learningnets