IT 18.01: Router Configuration Standards

Policy Authority

BTS Administrative Rule 2.2 Roles and Responsibilities
BTS Administrative Rule 2.16 Payment Card Security Standards

Purpose

In order to minimize the possibility of unauthorized access and/or control of City routers, certain minimum configuration standards for network devices are necessary.

Policy

Internal Network Devices Configuration Standards

The City of Portland Internal Network is a TCP/IP local area network (LAN) which is separated from the Internet by firewalls.

Internal network devices are TCP/IP network devices such as routers and switches which are physically located on the City of Portland internal LAN and protected by the firewalls. All internal network devices should be configured to the following minimum standards:

IP Addressing Standards

- Networks addressing
    - Internal networks use private network addresses as defined by Request for Comment (RFC) 1918.
- Management IP addresses
    - Internal Network Devices have an IP address for remote administration

Routing Protocol Standards

- IP Routing Protocol
    - Exterior Interior Gateway Routing Protocol (EIGRP) is the internal routing protocol
    - Routes are summarized, where practical, to reduce routing table size and complexity.
    - Default routes are the only routes advertised to EIGRP stubs.
    - Source routing is not allowed
- Static Routes
    - Static routes are allowed in cases where it is impractical to implement a routing protocol
- Multicast - The City of Portland utilizes:
    - IP Multicast routing
    - Protocol independent multicasting (PIM) in sparse-mode
    - Rendezvous Point (RP) for PIM

Unneeded Services

- All unneeded services are disabled, including but not limited to:
    - Hyper Text Transfer Protocol (HTTP)
    - Secure Hyper Text Transfer Protocol (HTTPS)
    - Telnet
    - PAD (packet assembler/disassembler commands)
    - Finger
    - Bootstrap Protocol (Bootp)
    - Uniform Datagram Protocol (UDP) and Transmission Control Protocol (TCP) small servers
    - Trivial File Transfer Protocol (TFTP)
    - Cisco Discovery Protocol (on external interfaces)
- Secure Shell (SSH) on TCP port 22 is the only allowed service for inbound connections
- Cisco Discovery Protocol (CDP) is allowed on ports that uplink to other City of Portland network devices
    - Each CDP uplink port shall have a description that includes the name of the remote device.

Configuration Maintenance

- Secure Copy (SCP) is the approved protocol for configuration file copies to and from network devices.
- PCI-DSS devices are configured to report to the Tripwire server and the Juniper Security and Threat Response Manager (STRM).
- Running configurations are synchronized with startup configurations daily

Authentication & Encryption

- All network devices utilize Cisco Terminal Access Controller Access- Control System (TACACS) for authentication.
- Cisco Access Control Server (ACS) controls all authentication requests.
- No shared accounts are allowed in ACS.
- A predefined unauthorized access warning notice is configured on each device through ‘banner message of the day (motd)’ functionality.

Password Settings

- Network team account passwords on the ACS appliance are changed at least every 90 days.
- Cisco Enable passwords are changed at least every 90 days.
- Account passwords shall comply with BTS Administrative Rule 2.05- User and Administrative Passwords.

Password Encryption

- Service password encryption is enabled using MD5.
- Network devices are configured with a key shared with the ACS server. This key is encrypted.

Management Access

- SSH version 2 is the approved protocol for remote access to network devices. All network devices require SSH to be used for remote access.
- All devices are set to time out any remote access after 10 minutes of inactivity
- Simple Network Management Protocol (SNMP) version 2 is the approved protocol for management of network devices.
    - SNMP write is not allowed
    - SNMP is configured for read only polling
    - SNMP statements are configured to define the device chassis-id,

contact information, and location for the device
- Network time protocol (NTP)
    - All network devices, except core routers, pull time from a internal core router acting as a stratum 2 clock
    - Core routers pull time from a stratum 1 clock

Logging
- All network devices:
    - are configured to log to a Syslog server
    - have one interface specified as a source interface
    - are configured to use localtime for 'log' and 'debug' timestamps
    - are configured to log up to informational (level 6) events

Network Segmentation
- Virtual Local Area Network (VLAN) configuration
    - VLANs are not trunked across the network core when at all possible.
    - Dynamic Host Control Protocol (DHCP) IP helper statements are configured on VLANs with client workstations
    - VLAN Trunk Protocol (VTP) is set to transparent.

General Device Standards
- All ports
    - Bridge Protocol Data Unit (BDU) Guard is enabled on all ports to prevent unauthorized connection of other spanning tree devices.
- Client access ports
    - Each server port has an informative description
    - Spanning-tree portfast is set on Client and Server ports
    - Client access ports are set to access mode to prevent trunk establishment

Edge Network Devices Configuration Standards

Edge Network Devices are defined as Routers and Switches with routable Internet Addresses positioned outside the City of Portland Firewalls.

Edge Network Devices Configuration Standards are in addition to/specific to Edge Devices. Unless otherwise noted all standards from Internal Network Devices Configuration Standards apply.

IP Addressing Standards
- Networks addressing
    - External network devices use addresses in the 209.162.223.0 and 69.30.62.8 spaces.

Routing Protocol Standards
- External Routing Protocol
    - Border Gateway Protocol v4 (BGP) is used between City of Portland routers and ISP upstream routers.
    - BGP routers use password authentication to communicate with BGP neighbor routers
- Internal Routing Protocol
    - Open Shortest Path First (OSPF) is used for routing between the edge routers, the edge switches, and the firewalls.
    - The City of Portland OSPF routers use MD5 message-digest authentication to communicate with OSPF neighbor routers.

- A layer 2 connection to the Police Bureau does not participate in OSPF. That interface is configured in passive mode (no OSPF announcements are sent).

Network Segmentation

- VLAN configuration
  - No DHCP IP helper statements are configured on any edge device

General Device Standards

- Router ports
  - Router Interfaces not in use are shut down administratively
  - DMZ interfaces not in use are shut down administratively
- Control Plane Policing (CoPP)
  - Control plane policing is a filter that protects the control plane of Cisco IOS routers and switches. BTS utilizes the following document as its configuration guidance for COPP: http://www.cisco.com/web/about/security/intelligence/coppwp_gs.html
  - Using CoPP, the following traffic types are classified into Categories and Rate Limited or dropped:
    - BGP
    - OSPF (the edge Interior Gateway Protocol (IGP))
    - Management traffic - SSH, telnet, NTP, SNMP, TACACS, TFTP, File Transfer Protocol (FTP)
    - Monitoring traffic – Internet Control Message Protocol (ICMP) echo and traceroute
    - Layer 2 Protocols – Address Resolution Protocol (ARP)
    - Undesirable – traffic that is dropped entirely; known bad ports
    - Default, unclassified traffic
- Access Control Lists (ACLs)
  - ACLs are configured as per Cisco best practices to drop harmful traffic (See Cisco best practices document http://www.cisco.com/web/about/security/intelligence/protecting_bgp.html)
    - RFC 1918 addresses are dropped on the Edge BGP devices
    - BGP traffic is dropped if not from specified neighbors
    - TCP and UDP fragments are dropped from BGP neighbors
    - Only BGP traffic is allowed from BGP neighbors.
    - TCP and UDP fragments are dropped from any source on the 209.162.223.0 and 69.30.62.8 address spaces (assigned address space)
    - ICMP fragments are dropped
    - Telnet is dropped from any source
    - Traffic from addresses 0.0.0.0 and 127.0.0.0 are dropped
    - Multicast packets are dropped
    - SNMP traffic not specifically allowed is dropped
    - Traffic to Edge 3750 is dropped
    - Traffic to Police Edge device is dropped
    - Inbound traffic purporting to come from 209.162.223.0 or 69.30.62.8 address spaces is dropped.
    - SSH traffic to edge devices from the internet is dropped.

Process

Configuration Maintenance

- Network devices' running configurations are synchronized with startup configurations

Authentication

- In order to ensure a highly available authentication infrastructure, BTS maintains dual Cisco ACS appliances to provide TACACS service.

Password Settings

- Network Engineering sets and maintains calendar reminders to rotate ACS passwords every 90 days.

Management Access

- Network Engineering maintains an access control list to ensure that only authorized devices pull read only SNMP data from network devices.

Password Encryption

- If any device with the shared key is lost or stolen, a new shared key is created and copied to every device.

Revision History

Version	Effective Date	Authored By	Approved By	Date
1.0	3/31/09	Neal Bialostosky, Network Engineering and Logan Kleier, Information Security	BTS Network Engineering & Information Security	4/14/09