

CCIE Security Lab Exam Outline (2006)

Bridging & Switching	1
IGP Routing	2
BGP	4
PIX Firewall	5
VPN	7
AAA	9
IP/IOS Features	10
IOS Firewall	11
Network Attack Mitigation	12
IDS	13

Bridging & Switching

- Frame-Relay
 - Interface Types
 - Point-to-Point
 - Multipoint
 - Physical
 - Address Resolution (Mappings)
 - Static
 - Dynamic
 - LMI, Interface Signalling Type (DTE/DCE/NNI)
- Catalyst 3550
 - VTP (modes and authentication)
 - Trunk allowed VLANs (Filtering)
 - Network Security with ACLs
 - Port Access-Lists (IP/MAC, Inbound)
 - Router ACLs
 - VLAN Access-Maps (IP/non-IP Filtering)
 - Compatibility and Performance Issues
 - Port Traffic Control
 - Port Security
 - Violate Actions (Shutdown, Restrict, Protect)
 - Errdisable recovery from psecure-violation
 - Sticky Addresses
 - Address Aging
 - Storm-Control (Unicast/Broadcast/Multicast)
 - Protected Ports
 - Unknown unicast/broadcast traffic
 - Spanning-Tree Protocol
 - Root-Bridge Election
 - Designated Bridge/Root-Port Election
 - Spanning-Tree Features
 - BPDU Guard/Filter
 - Root/Loop Guard
 - Portfast/BackboneFast/UplinkFast

- Timers Tuning (Fwd, MaxAge, Hello)
- Load-Balancing
 - Port Cost
 - Port Priority
 - VLAN filtering
- CAM/TCAM Maintenance (static MAC, drop)
 - SDM Preferences
- Errdisable
 - Errdisable Recovery Cause
 - Recovery Timer
- EtherChannels
 - LACP/PagP/Static
 - L3/L2
- Configuring SPAN and RSPAN
 - Reflector port
 - RSPAN VLAN
- 802.1x
 - Guest VLAN
 - Multi-host mode
 - Port Authorization
 - AAA issues (console authentication)
- QoS
 - Classification and Marking
 - Per-Port/Per-VLAN
 - ACLs
 - Trust (CoS, DSCP, IPP)
 - Translation Maps (DSCP)
 - Traffic Policing
 - Inbound (ACLs)
 - Outbound (DSCP only)
 - DSCP Markdown
 - Aggregate Policer
 - WRR Queue configuration
 - Weights
 - Drop Thresholds
 - Buffers Tuning (Min Reserve Levels)
 - CoS-to-Queue Maps
 - DSCP-to-Threshold Maps
 - Priority Queue
 - WRED on Gigabit Ports

IGP Routing

- OSPF
 - Establishing Adjacencies (MTU problems)
 - Network Types (Broadcast, NBMA, P2MP, P2P)

- Timers
 - Compatibility
- Adjacency Authentication
 - MD5/Text/Null
 - Area/Interface
 - MD5 Key Rollover
- Area Types (Regular, Stub, NSSA, No-Summary)
- Summarization/Area Ranges
- Route Filtering
 - Distribute-Lists
 - Local RIB Filtering
 - ASBR Outbound Filter
 - Inbound With Route-Map
 - Area LSA-3 Filters
 - Summarization/Ranges with No-Advertise keyword
 - NSSA ABR Summarization (7to5 Translator)
- Virtual-Links (Area 0 Authentication Issues)
- Path Selection (O/IA/E1/E2)
- RIP
 - Route Filtering
 - Distribute Lists (Standard/Extended, Prefix/Gateway)
 - Offset Lists
 - Summarization (Auto-summary, Manual)
 - Changing next-hop with summarization
 - Split-Horizon Issues
 - Unicast/Broadcast/Multicast Updates
 - TTL 2 for Unicast Updates
 - Authentication (Text/MD5)
 - RIP Timers Tuning
 - Update/Holddown/Invalid/Flush
- EIGRP
 - Authentication
 - Time-based Key Rotation
 - Route Filtering (Distribute-List, Offset-List)
 - Summarization (Auto-Summary)
 - Stub-Router feature
 - Split-horizon, Unicast Updates
 - Path Selection, EIGRP Metric
- PIX Routing
 - OSPF
 - Authentication (MD5/Text, Interface/Area)
 - Multiple OSPF Processes
 - OSPF Redistribution, Route-Maps
 - RIP (Passive/Default)
 - Static routes
- VPN3000 Routing
 - OSPF

- Router-ID
- Enabling Globally/Per-Interface
- Authentication (MD5/Text)
- Autonomous-System Feature
- HoldDown Routes
- Summary-LSAs
- Configuring Routing on Public Interface
- RIP
- Static (Interface/Router)
- Hold-Down Routes
- Policy Routing
 - Local Policy
 - PBR with 3550
- Route Redistribution
 - Tagging and Filtering
 - Route-Maps
 - Distribute-Lists
 - Prefix-Lists
 - Routing Loop Prevention

BGP

- Establishing Peering
 - Session Initiation
 - Default-route only and eBGP
 - Single-side Initiation (through PIX)
 - eBGP Multihop Issues
 - Update Source
 - MD5 Authentication
 - General NAT and PIX NAT issues
- iBGP
 - Synchronization
 - OSPF RID issues
 - Route-Reflectors (Cluster-ID)
 - Confederations
 - Next-Hop Processing
 - Next-Hop-Self
 - Next-hop Peer Address
 - Set IP next-hop
- Best-Path Selection
 - Valid Next-Hop
 - Local Preference
 - AS-PATH Prepend
 - Metric Manipulation
 - AS-PATH Ignore Option
- BGP Summarization

- Aggregate Address
 - Summary-only
 - Suppress Map
 - Suppress Map (per peer)
 - AS-SET
 - Attribute Map
 - Advertise Map
- Redistribution
 - iBGP Redistribution
- BGP Filtering
 - Distribute-Lists/Prefix-Lists
 - Route-Maps
 - Filter-Lists (AS-PATH Regexprs)
 - Well-Known Communities (No-Export, No-Advertise, Internet)
 - Remove Private-AS
 - Allow AS in
 - Max AS Limit
- BGP Conditional Route Advertisement
 - Exist/Non-Exist Map
 - Advertise Map
- Local AS (No-Prepend)
- BGP Load-Balancing
- BGP Dampening
 - Tuning Dampening with Route-Map
- BGP Table Map and QPPB

PIX Firewall

- Basic Configuration
 - Interfaces Naming, Security Levels, IP Addressing
 - VLANs
- Establishing Connectivity
 - Configuring Routing
 - NAT
 - Dynamic NAT/PAT (nat/global)
 - Identity NAT (nat 0)
 - NAT Exemption (nat 0 access-list)
 - Static (+Port Redirection)
 - Policy NAT
 - Outside NAT
 - Outside NAT issues
 - DNAT/Alias (DNS doctoring)
 - Static with DNS keyword
 - TCP Intercept features
 - IPSec and NAT
 - NAT Exemption

- PL-Compatible
- Network Access Control
 - Access-Lists
 - Conduits
 - Outbound/Apply
 - Established/Permitto
 - Object Groups
 - Network
 - ICMP types
 - Ports (TCP/UDP)
 - HTTP Control
 - URL Filtering (Websense/N2H2)
 - Java/ActiveX Filtering
 - uRPF
- Stub Multicast Routing
 - IGMP Forwarding
 - Static Mroutes
- Device Administration
 - Remote Access
 - Configuring Users and Passwords
 - SSH
 - Telnet
 - IPSec & Telnet on outside
 - HTTPs/PDM configuration
 - SNMP
 - Logging Configuration
 - Remote
 - Buffered
 - NTP
 - NTP Authentication
- PIX SOHO Environment Features
 - DHCP
 - DHCP Server
 - DHCP Relay
 - DHCP Outside Address Configuration
 - PPPoE Client
 - ezVPN Client (Client/Network Extension modes)
- Protocol Fixups
 - ESMTTP issues
 - FTP issues
 - Disabling Fixups
- Sysopts
 - Permit IPSec/PPTP/L2TP
 - TCP Timewait/TCP MSS
 - ProxyARP/DNS Alias
- Service ResetInbound/ResetOutside

VPN

- General ISAKMP/IKE
 - ISAKMP identity
 - Address
 - Hostname
 - DN
 - Peer Authentication
 - Pre-Share
 - Wildcard key
 - KeyRing
 - RSA-Encryption
 - Exporting/Importing RSA Keys
 - RSA Keyrings
 - RSA-Signatures
 - Configuring CA Interoperability (PIX/IOS/VPN3000)
 - RSA Key Generation
 - CA URL
 - Enrolling with CA
 - Handling CRLs
 - ISAKMP Profiles
 - Identity matching
- General IPsec
 - Configuring Transform-Sets
 - Static Crypto Maps
 - Dynamic Crypto Maps
 - DN-based Crypto Maps (IOS)
 - TED (IOS)
 - Passive IPsec Mode (IOS)
 - IPsec High Availability
 - IPsec and HSRP (IOS)
 - RRI (IOS)
 - Local-Address (IOS)
 - Multiple Peers
 - IPsec SA Idle Timer (IOS)
- LAN-to-LAN
 - IPsec Tunnels (IOS, PIX, VPN3000)
 - IPsec NAT-T
 - NAT with IPsec
 - Host-to-Host (IPsec Transport)
 - GRE Tunnels over IPsec & IPsec profiles (IOS Routers)
 - Routing with IPsec/GRE Tunnels
- VPN3000
 - Device Administration
 - Events and Logging
 - Management Protocols (HTTP, HTTPS, SNMP, TFTP, FTP)

- VPN3000 Web GUI/CLI
- Configuring Addressing
 - Local Pools
 - Global
 - Group-Specific
 - DHCP Relay
- Users & Groups
 - Remote Authentication
 - Remote Authorization
- Group Policies
 - Traffic Filters and Rules
 - Bandwidth Reservation Policies
- NAT
 - LAN-to-LAN
 - Dynamic
- PPTP/L2TP
- WebVPN
 - Static URLs
 - Access-control and URL Filtering
 - Application Port Redirection
 - IMAPs/POP3s/SMTPs Proxy
- Remote Access VPN
 - VPDN
 - PPTP/L2TP Access Server (PIX/VPN3000/IOS)
 - L2TP over IPsec
 - ezVPN
 - Client Mode
 - NAT
 - Dynamic address allocation
 - Network Extension Mode
 - Compatibility Issues (DH Group2)
 - IOS ezVPN Server
 - RRI
 - Xauth: AAA User Authentication
 - Local
 - Remote
 - Disabling Xauth for Static Peers
 - Group Authorization with AAA Server
 - Address Pools
 - Split-tunneling and Split-DNS
 - PIX ezVPN Server
 - Static Route to Remote Address Range
 - VPN3000 ezVPN Server
 - RRI
 - HoldDown Routes
 - IOS ezVPN Remote (Client/Network Extension modes)
 - PIX ezVPN Client (Client/Network Extension modes)

- Cisco VPN Client
 - Group Authentication with Certificates/Pre-Shared Key
 - Enrolling with CA
 - IPsec over NAT/TCP
- DMVPN
 - mGRE
 - NHRP
 - Static Mappings
 - Hold-Time
 - Registration
 - Dynamic Mappings
 - DMVPN Routing
- Combining Multiple VPN types on single device
 - ISAKMP profiles
- VPN QoS
 - Pre-Classify (GRE, IPsec, Virtual-Template)
 - IPsec Fragmentation Policy
 - ToS byte copy to Tunnel header
 - VPN3000 QoS Features
 - Policing
 - Bandwidth Reservation

AAA

- AAA Servers (RADIUS/TACACS+)
 - Configuring AAA servers (PIX/IOS/VPN3000)
 - Configuring named AAA lists (PIX/IOS)
- Device Access
 - Login Authentication (VTY, Console, HTTP)
 - HTTP/Console Authentication Issues
 - Shell (Exec) Authorization on PIX/IOS
 - Exec Authorization Issues with 3550
 - Command Accounting (IOS)
 - Local/Remote Command Authorization on PIX/IOS
- Network Access
 - PIX Service Authentication
 - Include
 - Match Access-List
 - PIX/TACACS+ Service Authorization
 - Shell Command Authorization Sets
 - PIX Virtual HTTP/Telnet Server
 - Configuration Static
 - IOS Authentication Proxy
 - Cache expiration timeouts
 - Downloadable ACLs (RADIUS/PIX)
 - Filter-ID (ACL name) attribute

- Cisco AV-Pair
- Downloadable ACL
- Network Authorization and Accounting
- Remote Access AAA
 - PPP AAA (PPTP/L2TP)
 - PPP Authorization
 - ezVPN AAA (Xauth, Group Authorization)

IP/IOS Features

- IP Services
 - ICMP (Rate-Limiting and Message Types)
 - DHCP/BOOTP
 - Server configuration
 - Client/Interface Addressing (Client-ID)
 - DHCP Relay, Information Option
 - IPCP Addressing via DHCP
 - DHCP Proxy
 - Multiple Gateways for Redundancy
 - TCP/UDP Small Services
 - Helper Address, Broadcast Forwarding, HSRP Redundancy
 - ARP/Proxy ARP/Local Proxy ARP
 - HSRP/VRRP (Gateway Redundancy)
 - Preemption
 - Authentication
 - Interface/Object Tracking
 - NetFlow
 - Accounting
 - Access-Violation
 - Output Packets
 - Precedence
 - WCCP/DRP
 - Gateway Discovery Protocols (IRDP)
- QoS
 - Classification and Marking
 - MQC
 - Precedence/DSCP
 - FR DE bit
 - Packet Length
 - ACLs
 - NBAR
 - Custom Protocols, Port Mapping
 - Matching URLs, MIME-types, Host Field with HTTP
 - Traffic Flow Control
 - Policing (MQC/CAR)
 - Shaping

- GTS
 - MQC Class-Based
 - FRTS
 - Legacy
 - MQC
- Congestion Management/Avoidance
 - Fancy Queueing (WFQ/CQ/PQ)
 - CBWFQ/LLQ
 - WRED (Legacy/MQC)
 - FrameRelay Queueing and Fragmentation
- IOS NAT
 - Inside/Outside, Overload (PAT)
 - Destination (Rotary Pools)
 - Route-maps with NAT
 - Static Translations/Port Redirection
 - Static Network Translation
 - Stateful NAT
 - On a Stick
- System Management
 - SDM
 - NTP
 - SNMP
 - Generating Traps & Informs
 - Communities and Basic Access Control
 - SNMPv3 Access Control
 - Telnet/SSH VTY access
 - Rotary Groups
 - File Management
 - HTTP/HTTPs Server
 - TFTP/FTP Server and Client
 - Menus and Banners
 - Terminal Lines
 - Reverse Telnet/SSH
 - Troubleshooting and Logging
 - Exceptions
 - Core Dumps
 - Syslog
 - AutoInstall (SLARP/BOOTP/DHCP)

IOS Firewall

- Access-Lists
 - Standard/Extended/Named
 - Filtering Fragments
 - Established TCP Sessions
 - Port Ranges

- Reflective ACLs
 - Processing Self-Generated Traffic
- Dynamic-ACLs (Lock & Key)
 - Absolute/Idle Timeouts
 - Dynamic-Extended
- Access-Classes (VTY, SNMP, HTTP)
- Time-Ranges
 - Periodic
 - Absolute
- CBAC
 - Timeouts (TCP/UDP/DNS)
 - TCP Intercept Feature (Thresholds)
 - HTTP Java/URL filtering
 - PAM
 - Access-List
- Legacy TCP Intercept
 - Watch Mode
 - Intercept Mode
- uRPF
 - Loose Mode
 - Exceptions

Network Attack Mitigation

- Monitoring Network Traffic Flows
 - NetFlow
 - Accounting
 - ACL Logging
- Flooding Attack/Network Worms Mitigation (Smurf/Slammer)
 - Packet Classification and Marking (MQC/NBAR)
 - Counter-Measures
 - Traffic Policing (MQC/CAR)
 - Priority Queueing (LLQ/CBWFO)
 - PBR
- SYN-Flooding
 - TCP Intercept
- DDoS Attack Mitigation
 - BGP Blackhole routing
 - Source-Based
 - Destination-Based
 - Sinkholes
 - Community signalling
 - MQC Policing/CAR
 - Single-Rate Policer
 - Two-Rate Policer
 - Legacy CAR
- Spoofing Attack Mitigation (BCP27, ACLs, uRPF)

- Network Device Hardening Best Practices

IDS

- 4200 IDS Appliance
 - Basic Configuration
 - Host Access Control
 - Usernames, Roles
 - SSH/Telnet (Known Hosts, Authorized Hosts)
 - HTTP/HTTPs
 - Network Access Control
 - Shunning
 - Configuring blocking for PIX/IOS devices
 - Telnet/SSH device access
 - Master Blocking Sensor
 - IEV
 - Adding Sensor
 - Adding Views
 - Tuning Filters
 - IDSM
 - Configuration
 - Administration
 - Monitoring
 - Sensing Engine
 - Tuning Existing Signatures
 - Creating Custom Signatures
 - Tuning Packet/Flow Reassembly Options
- IOS IDS
 - Configuring PO Parameters
 - Disabling Signatures
 - Limiting Signature Scope
 - Configuring SPAM Blocking
 - Configuring Info/Attack Actions
- PIX IDS
 - Configuring Info/Attack Actions
 - Disabling Signatures