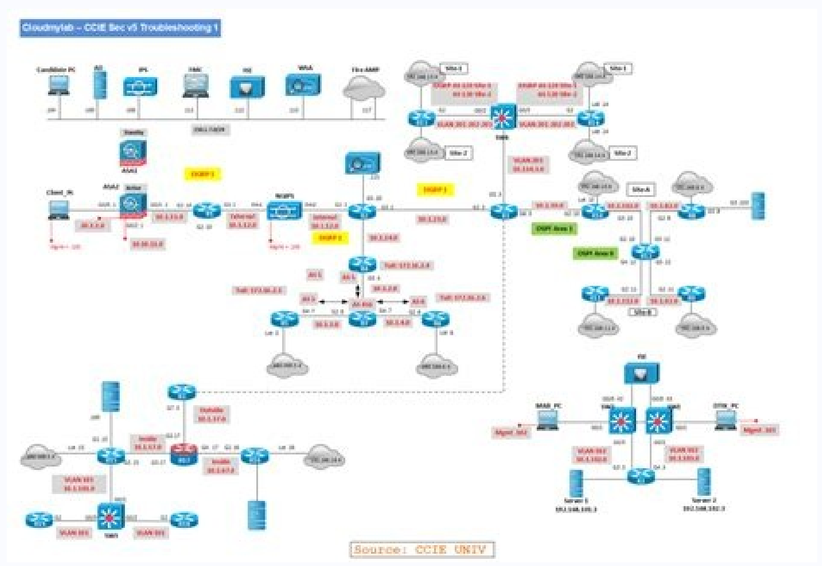
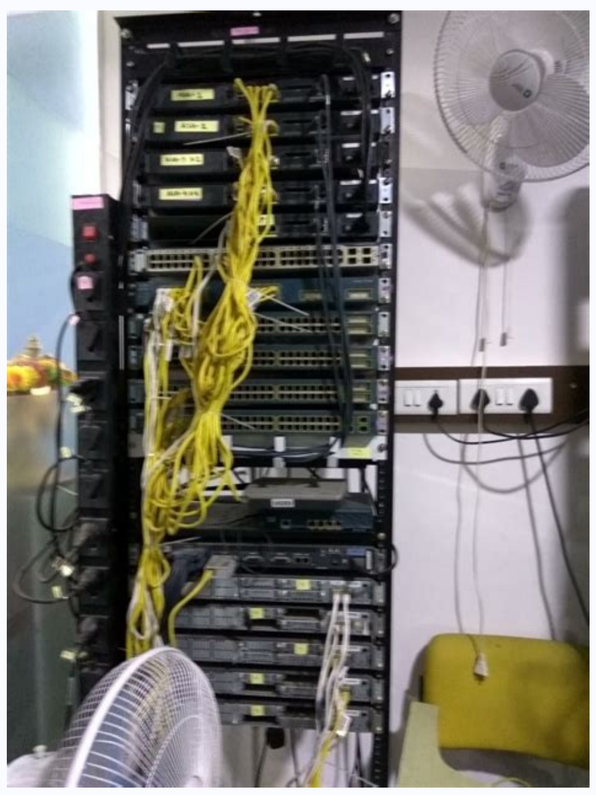
Ccie security v5 books pdf

I'm not robot!





CCIE Security Book List

This page intends to list all books appearing on the CCIE exam blueprints. These books are not required study resources, however, they can be used to build knowledge in certain areas.

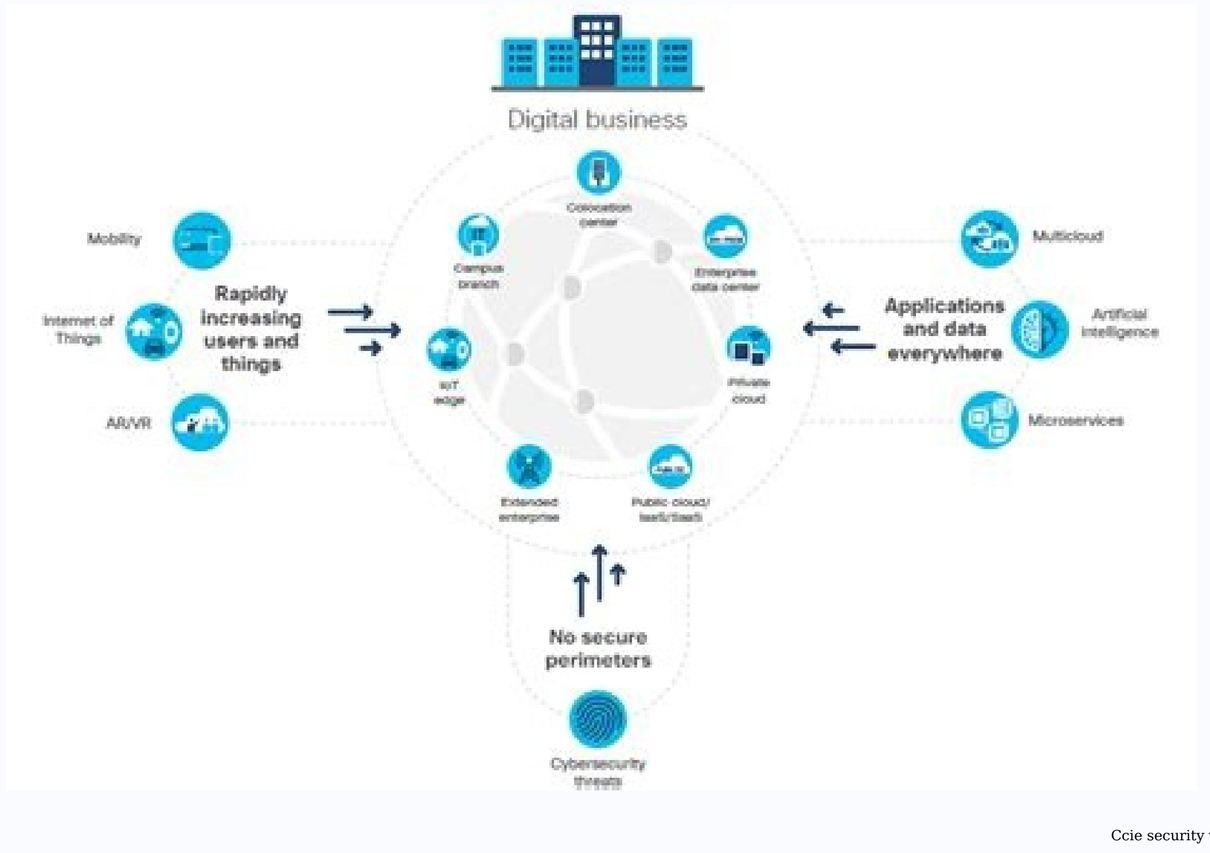
The books reviewed (Bold) published by Cisco Press, as well as others known to CCIE program managers. Many of the Cisco Press books are available to certified individuals and Cisco customers at prices discounted up to 35% off. To view the discounts, visit the Cisco Marketplace. Join or (Cisco Press) Bookstore, and login with your Cisco CCO ID. Search for the titles listed below to see the discount available.

Cisco Press Titles

- IBM Security Management Security (Kahlera, Bangs, Carroll, ISBN-1-59714-154-3)
- CCIE Security v5.0 Configuration Lists (Various authors/editors, ISBN# 9781542393)
- CCIE Security v5.0 Configuration Lists (Various authors/editors, ISBN# 9781542393)
- Cisco ASA: All-in-One Firewall, IPS, Anti-X, and VPN Adaptive Security Appliance, 2nd Edition (Frahim, Santos, ISBN# 1587143070)
- Cisco Firewalls: Concepts, design, and deployment for Cisco Stateful Firewall solutions (Alsaadi, ISBN# 1587141566)
- Cisco Network Security Troubleshooting (Hancock and Jones, ISBN# 1587059030)
- Cisco Secure Intrusion Detection System (Northcutt, Cooper, Fearnow, ISBN# 1587130939)
- Cisco Secure Virtual Private and Extranet (Pohlmann, Strothi, Morrow, Berg, ISBN-1-58705-810-7)
- Designing Network Security, Second Edition (Kaeo, ISBN# 1587051176)
- End-to-End Network Security (Kalman, ISBN# 1587051583)
- Implementing Cisco IOS Network Security (IINS 640-554) (Foxpen, ISBN-1-58714-214-4)
- IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6 (Graziani, ISBN-1-58714-314-0)
- Network Security Architectures (Sherif, Cocker, ISBN# 1587052458)
- Office VPN Design (Bollapragada, Khalid, Palkar, ISBN# 1587051311)
- PIX Security (Hwang, Vanno, ISBN# 1587050943)
- Router Security Strategies (Murphy, ISBN# 0072253916)
- Software Security Technologies and Solutions (Wang, ISBN# 1587053454)
- Translation Testing and Network Defense (Greenlee, Whitaker, ISBN# 1587053292)
- Troubleshooting Virtual Private Networks (Vese, Lee, ISBN# 1587051796)
- Routing in the IPv6 Internet, Second Edition (Huston, Savola, ISBN# 0470010634)
- Routing TCP/IP, Volume 2 (Doyle, Dehaven Carroll, ISBN# 1578700892)
- Securing Cisco IP Telephony Networks (Behl, ISBN-1-58714-280-5)
- Troubleshooting Virtual Private Networks (Vese, Lee, ISBN# 1587051796)
- Troubleshooting IP Routing Protocols (Wei Lee, Moore, Pillay, ISBN# 1587052032)

Other Publications

- Network Security Architectures (Hord and Kaeley, McDermott, ISBN#0201433362)
- Firewalls and Internet Security, Second Edition (Cheswick, Bellovin, and Rubin, Addison-Wesley, ISBN# 0201633574)
- Internetworking with TCP/IP Volume I Principles, Protocols, and Architecture (4th Edition) (Comer and Stevens, Prentice Hall, ISBN# 0130183806)
- Internet Security Protocols: Protecting IP Traffic (Black, Prentice Hall, ISBN# 0130142921)



Ccie security v5 vs v6. Ccie security v6 book.

Full PDF PackageDownload Full PDF PackageThis PaperA short summary of this paper4 Full PDFs related to this paperDownloadPDF Pack Trust the best selling Official Cert Guide series from Cisco Press to help you learn, prepare, and practice for exam success. They are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, Fifth Edition from Cisco Press enables you to succeed on the exam the first time and is the only self-study resource approved by Cisco. Expert instructors Narbik Kocharians and Terry Vinson share preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. This second of two volumes covers IP BGP routing, quality of service (QoS), wide area networks, IP multicast, network security, and Multiprotocol Label Switching (MPLS) topics. This complete study package includes -- A test-preparation routine proven to help you pass the exams -- Do I Know This Already? quizzes, which enable you to decide how much time you need to spend on each section -- Chapter-ending exercises, which help you drill on key concepts you must know thoroughly -- The powerful Pearson IT Certification Practice Test software, complete with hundreds of well-reviewed, exam-realistic questions, customization options, and detailed performance reports -- A final preparation chapter, which guides you through tools and resources to help you craft your review and test-taking strategies -- Study plan suggestions and templates to help you organize and optimize your study time Well regarded for its level of detail, study plans, assessment features, challenging review questions and exercises, this official study guide helps you master the concepts and techniques that ensure your exam success. The official study guide helps you master topics on the CCIE Routing and Switching v5.0 exams, including: -- BGP operations and routing policies -- QoS -- WANs -- IP Multicast -- Device and network security and tunneling technologies -- MPLS CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, Fifth Edition is part of a recommended learning path from Cisco that includes simulation and hands-on training from authorized Cisco Learning Partners and self-study products from Cisco Press. To find out more about instructor-led training, e-learning, and hands-on instruction offered by authorized Cisco Learning Partners worldwide, please visit www.cisco.com/go/authorizedtraining. The print edition of the CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2, Fifth Edition contains more than 200 practice exam questions. Also available from Cisco Press for Cisco CCIE R&S v5.0 study is the CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2 Premium Edition eBook and Practice Test, Fifth Edition. This digital-only certification preparation product combines an eBook with enhanced Pearson IT Certification Practice Test. This integrated learning package: -- Allows you to focus on individual topic areas or take complete, timed exams -- Includes direct links from each question to detailed tutorials to help you understand the concepts behind the questions -- Provides additional unique sets of exam-realistic practice questions -- Tracks your performance and provides feedback on a module-by-module basis, laying out a complete assessment of your knowledge to help you focus your study where it is needed most This print book includes a 70% discount offer off the list price of the CCIE Routing and Switching v5.0 Official Cert Guide, Volume 2 Premium Edition eBook and Practice Test, Fifth Edition to help enhance your exam preparation experience. A comprehensive manual on how to prepare for the CCIE Security Lab exam uses seven complete hands-on lab scenarios that encompass all major exam subject areas, including security protocols, operating systems, application protocols, general networking, security technologies, Cisco security applications, and Cisco IOS software specifics. (Advanced) ×Sorry to interruptCSS Error CCIE Enterprise Infrastructure Foundation, 2nd EditionCCNA 200-301 Official Cert Guide, Volume 2 Premium Edition eBook and Practice TestIntegrated Security Technologies and Solutions - Volume II: Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and VirtualizationCCIE Wireless v3 Study GuideCCIE and CCDE Evolving Technologies Study GuideIntegrated Security Technologies and Solutions - Volume I: Cisco Security Solutions for Advanced Threat Protection with Next Generation Firewall, Intrusion Prevention, AMP, and Content SecurityCCIE Routing and Switching v5.1 Foundations: Bridging the Gap Between CCNP and CCIENetwork Security Technologies and Solutions (CCIE Professional Development Series)By Yusuf Bhaiji Published Nov 1, 2016 by Cisco PressBook $67.99eBook $53.59Routing TCP/IP, Volume II: CCIE Professional Development, 2nd EditionCCIE Collaboration Lab Exam LiveLessonsnewCCIE Enterprise Infrastructure Foundation, 2nd EditionBy Narbik Kocharians Published Jul 25, 2022 by Cisco PressBook $99.99eBook $79.99CCNA 200-301 Official Cert Guide, Volume 2 Premium Edition eBook and Practice TestBy Wendell Odom Published Dec 17, 2019 by Cisco PressPremium Edition eBook $35.99Integrated Security Technologies and Solutions - Volume II: Cisco Security Solutions for Network Access Control, Segmentation, Context Sharing, Secure Connectivity and VirtualizationBy Aaron Woland, Vivek Santuka, Chad Mitchell, Jamie Sanbower Published Apr 6, 2019 by Cisco PressBook $63.99eBook $51.19CCIE Wireless v3 Study GuideBy Carlos Alcantara, Nicolas Darchis, Jerome Henry, Jeal Jimenez, Federico Ziliotto Published Nov 27, 2018 by Cisco PresseBook (Watermarked) $119.99CCIE and CCDE Evolving Technologies Study GuideBy Brad Edgeworth, Jason Gooley, Ramiro Garza Rios Published Oct 31, 2018 by Cisco PresseBook (Watermarked) $95.99See All Titles Stuart Fordham June 14, 2016 CCIE, Security The current “official” CCIE Security reading list sucks. Hopefully, Cisco will update it, but there is a lot of older books on there, certainly not suitable for the new exam. In this post, I will list a few of the suitable books for the new exam. Some have not been released yet, and some are old, but are still extremely useful for both the CCIE Security written and lab exams. Do check out the Amazon marketplace, as there are some bargains to be had! CCIE Security v5 reading list FirePOWER Cisco Next-Generation Security Solutions: All-in-one Cisco ASA Firepower Services, NGIPS, and AMP Authors: Omar Santos, Panos Kampanakis, Aaron Woland ISBN: 978-1587144462 SSFIPS Securing Cisco Networks with Sourcefire Intrusion Prevention System Study Guide: Exam 500-285 Authors: Todd Lammle Alex Tatistcheff, John Gay ISBN: 978-1119155034 ASA Cisco ASA: All-in-one Next-Generation Firewall, IPS, and VPN Services (3rd Edition) Authors: Jazib Frahim, Omar Santos, Andrew Ossipov ISBN: 978-1587143076 IPv6 IPv6 Security Authors: Scott Hogg, Eric Vyncke ISBN: 061-9472055946 IOS/IOS-XR IP Routing on Cisco IOS, IOS XE, and IOS XR: An Essential Guide to Understanding and Implementing IP Routing Protocols Authors: Brad Edgeworth, Aaron Foss, Ramiro Garza Rios ISBN: 978-1587144233 ESA Email Security with Cisco IronPort Author: Chris Porter ISBN: 061-9472142929 ISE Practical Deployment of Cisco Identity Services Engine (ISE): Real-World Examples of AAA Deployments Authors: Andy Richter, Jeremy Wood ISBN: 978-0128044575 Cisco ISE for BYOD and Secure Unified Access Authors: Jamey Heary, Aaron Woland ISBN: 978-1587143250 ACS AAA Identity Management Security Authors: Vivek Santuka, Premdeep Banga, Brandon J. Carroll ISBN: 061-9472141441 NetFlow/IPFIX Network Security with NetFlow and IPFIX: Big Data Analytics for Information Security Author: Omar Santos ISBN: 978-1587144387 VPNS: GETVPN, FlexVPN, DMVPN etc The Complete Cisco VPN Configuration Guide Author: Richard Deal ISBN: 978-1587052040 IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS Authors: Graham Bartlett, Amjad Inamdar ISBN: 978-1587144608 VPNs and NAT for Cisco Networks Author: Stuart Fordham ISBN: 978-1507646588 ACI, EVPN, VXLAN, NVGRE Building Data Centers with VXLAN EVPN Authors: Lukas Krattiger, Shyam Kapadia, David Jansen ISBN: 978-1587144677 The Policy Driven Data Center with ACI: Architecture, Concepts, and Methodology Authors: Lucien Avramov, Maurizio Portolani ISBN: 978-1587144905 General Router Security Strategies: Securing IP Network Traffic Planes Authors: Gregg Schudel, David Smith ISBN: 061-9472053362 LAN Switch Security: What Hackers Know About Your Switches Authors: Eric Vyncke, Christopher Paggen ISBN: 061-9472052563 IoT IoT Fundamentals: Networking Technologies, Protocols, and Use Cases for the Internet of Things Authors: David Hanes, Gonzalo Salgueiro, Patrick Grossetete, Subodh Gajare ISBN: 978-1587144561 SDN Programming and Automating Cisco Networks: A guide to network programmability and automation in the data center, campus, and WAN Authors: Ryan Tischer, Jason Gooley ISBN: 978-1587144653 CCIE Security v5 Authored By: Khawar Butt Hexa CCIE # 12353 (R/S, Security, SP, Voice, Storage,Data Center) CCDE # 20110020 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 1 of 404 Table of Contents Virtual Private Networks [VPN] Page Module 1 – Basic VPNs LAN-To-LAN Tunnel without NAT-T LAN-To-LAN Tunnel with NAT-T Point-to-Point GRE Encrypting GRE Tunnels using IPSec Configuring a Native IPSec Tunnel Interface using StaticVirtual Tunnel Interface (S-VTI) Module 2 – Advanced VPNs Multipoint GRE (mGRE) Tunnel Configuring DMVPN – Phase I Configuring DMVPN – Phase II Configuring DMVPN – Phase III Configuring DMVPN Phase III with Dual Hub Encrypting DMVPN Traffic using IPSec Configuring GETVPN Configuring GETVPN with Redundancy Configuring VRF aware VPN Configuring a Router as a CA Server

EZVPN – Client Mode EZVPN – Network Extension Mode Module 3 – Configuring VPNs using IKEv2 Site-To-Site IPSec VPN using IKEv2 – Crypto Maps Site-To-Site IPSec VPN using IKEv2 – S-VTI Module 4 – Configuring Flex VPNs Site-To-Site IPSec VPN using Flex VPN Spoke-To-Spoke IPSec VPN using Flex VPN Server – Client IPSec Flex VPN Configuring Router & Switch Security Features Module 1 – Control Plane Management Configuring Control Plane Policing Configuring Control Plane Protection for Port Filtering Module 2 – Configuring Router Security Features Configuring Anti-Spoofing ACLs & the RPF Feature Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 2 of 404 Configuring NTP with Authentication Configuring the Router for SNMP Blocking Unwanted Services on the Router Configuring Syslog Settings Module 3 – Configuring Switch Security Features Configuring the Port-Security Feature on the Switch Preventing the Rogue DHCP Server Attack using the DHCP Snooping Feature Configuring Static ARP Inspection Using an ARP ACL Configuring Dynamic ARP Inspection (DAI) Configuring the Source Guard Feature Configuring VLAN ACL’s Module 4 – Configuring IPv6 Configuring Configuring Configuring Configuring Configuring IPv6 with RIPng IPv6 with EIGRP IPv6 with OSPFv3 IPv6 in IPv4 Tunnel a IPSec S-VTI Tunnel – IPv6 Configuring Firewalls, Intrusion Prevention & AMP Module 1 – Basic ASA Configurations on 9.X Page Initializing the FW Static and Default Routes Running RIP v2 Running OSPF Running EIGRP Configuring Management Protocols Module 2 – NAT & ACLs on 9.X Configuring Basic NAT Operations Configuring Static NAT, Static Identity NAT & Static PAT Configuring Destination NAT Configuring Twice-NAT Access Control Module 3 – Configuring High Availability Features Interface Redundancy Route Tracking using SLA Monitor Active/Standby Failover Stateful Failover Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 3 of 404 Security Contexts on the ASA using Shared Interface Active/Active Failover Port Channels Clustering – Interface Interface Mode Clustering – Spanning Interface Mode Module 4 – Deep Packet Inspection Configuring System L7 Deep Packet Inspection Configuring User Defined L7 Deep Packet Inspection Configuring TCP Normalization Module 5 – Transparent Firewalls on 9.X Configuring a Transparent Firewall Configuring Management on a Transparent FW ACL’s in Transparent Mode Configuring NAT on a Transparent Firewall Module 6 – Configuring the Firewall Component of FTD Initial Configuration of FTD & FMC from CLI Registering & Initializing the FTD device on FMC FTD Interface Configuration Routing Protocol Configuration - Static & Default Routes Routing Protocol Configuration – RIP Routing Protocol Configuration – OSPF Routing Protocol Configuration – BGP Configuring Access Control Policies – Basic Configuring Access Control Policies - Advanced Configuring Dynamic NAT Configuring Static NAT Configuring Dynamic PAT Configuring Static PAT Configuring Twice-NAT Module 7 – Configuring Intrusion Prevention Configuring a Balanced Intrusion Prevention Policies Tuning an Existing Signature on the Intrusion Policy Configuring an Event Filter Configuring a Custom Signature Configuring Network Discovery Policy Configuring an Intrusion Policy based on the Firepower Recommendations Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 4 of 404 Module 8 – Configuring AMP Configure AMP Policies to Block Specific File types Configure AMP Policies to Block Files Infected with Malware Module 9 – Configuring IOS-Based Firewall Configuring Zone-based Firewall on a Router Configuring Port-maps in Zone-based Firewalls Configuring Nested Classes in Zone-based Firewalls Module 10 – Configuring VPNs on ASA & FTD Configuring Configuring Configuring Configuring Configuring LAN-TO-LAN IPSec VPN on ASA – IKEv1 LAN-TO-LAN IPSec VPN on ASA – IKEv2 Remote-Access IPSec VPN on ASA Remote-Access SSL-Based VPN on ASA Clientless SSL VPN on ASA IPSec LAN-TO-LAN VPN on FTD – IKEv1 IPSec LAN-TO-LAN VPN on FTD – IKEv2 Configuring ACS 5.X Module 1 – Configuring ACS for Management Authentication Configuring a Router to Authenticate using the ACS Server Configuring a Switch to Authenticate using the ACS Server Configuring a Firewall to Authenticate using the ACS Server Module 2 – Configuring ACS for Management Authorization Configuring a Router for Exec Authorization Using the ACS Configuring a Router for Command Authorization Using the ACS Configuring ACS Authentication for HTTP Management on a Router Module 3 – Configuring ACS for Management Accounting Configuring Exec and Command Accounting on a Router Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 5 of 404 Configuring Exec Accounting on a Switch Configuring Telnet & SSH Connection Accounting Configuring WLC Module 1 – Initial Configuration of the WLC & WAP Basic Intialization of the Wireless LAN Controller (WLC) Basic Configuration of the Wireless Access Point (WAP) Using DHCP Module 2 – Configuring a Basic Wireless LAN Creating VLAN Interface on the WLC Configuring WLANs, SSID’s and associating them with VLAN Interfaces – Open Authentication Configuring WLANs, SSIDs and associating them with VLAN Interfaces – Static WEP PSK (40-Bit) Configuring WLANs, SSIDs and associating them with VLAN Interfaces – Static WEP PSK (104-Bit) Configuring SSID’s with Web Authentication Configuring ISE Module 1 – Configuring ISE to communicate to the Switch & WLC Network Devices Preparing the Network for ISE Basic Intialization of Identity Service Engine (ISE) Associating the Switch with the ISE Appliance Intializating & Associating the WLC with the ISE Appliance Module 2 – Configuring 802.1x using ISE Configuring 802.1x Authentication for a Wired Client Configuring 802.1x Authentication for a Wired Client with VLAN Assignment Configuring 802.1x Authentication for a Wired Client With DACL Assignment Configuring 802.1x Authentication for a Wireless Client with VLAN Assignment Configuring Wired MAB Authentication with VLAN Assignment Configuring Wireless MAB Authentication with VLAN Assignment Configuring Wired MAB Authentication for IP Phone & Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 6 of 404 Dot1X for PC behind it Module 3 – Configuring Posture Validation Using ISE Configuring Client Provisioning Resources & Policies Configuring Posture Validation based on Operating System & Anti-Virus Requirements Configuring Posture Validation based on Operating System & Application Requirements Module 4 – Configuring Cisco TrustSec with SGT Exchange Protocol [SXP] Configuring CTS SXP Relationship between ISE & the WLC & ASA Firewall Configuring SGT Group Setup on ISE Module 5 – Configuring ISE for Device Administration Configuring a TACACS+ relationship between ISE & Router/Switch Configuring ISE to support Device Administration Configure the Router & Switch to Use ISE for Authentication & Authorization Configuring Web Security Appliance [WSA] Module 1 – Initial Configuration of the WSA (Ironport) Basic Intialization of the Web Security Appliance (WSA) Ironport Configuring the ASA – WSA Relationship for WCCP Configuring the Router – WSA Relationship for WCCP Module 2 – Configuring Web Filtering Using WSA Creating Identities Used for Web Filtering Category Based Blocking on the WSA Blocking Custom URLs Blocking/Premiting Specific Identities Time-Based Blocking Configuring E-Mail Security Appliance [ESA] Module 1 – Initial Configuration of the ESA (Ironport) Initial E-Mail Server and Client Setup in the Network Initializing the ESA Appliance from CLI Initializing the ESA Appliance from GUI Using the System Setup Wizard Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 7 of 404 Configuring the ESA Appliance as a SMTP Relay Agent Module 2 – Configuring E-Mail Filtering Using ESA Configuring Incoming Filters Configuring Outgoing Filters Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 8 of 404 CCIE Security v5 – Advanced VPNs Module 1 – Basic VPNs Module 1 – Virtual Private Networks [VPN] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 9 of 404 Lab 1 – LAN-To-LAN Tunnel without NAT-T R1 F 0/0 (.1) 10.11.11.0/24 G 0/1 (.10) R4 192.1.40.0/24 ASA G 0/2 (.10) F0/0 (.4) 10.4.4.0/24 G 0/0 (.10) 192.1.20.0/24 F 0/0 (.2) R2 F 0/1 (.2) 192.1.23.0/24 F 0/0 (.3) 10.3.3.0/24 R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 10 of 404 Lab Scenario: Configure an IPSec LAN-to-LAN Tunnel from R4 to a Router on the Internet R3. R2 is your Perimeter Router. Open the appropriate Entries in the FW ACL to allow the tunnel to form Initial Setup: Configure the IP Addresses based on the Diagram. Set the Security Level of the DMZ interface (E2) on the Firewall to 50. Configure the following Static Routes on the appropriate routers: o o o o Default Routes on R1 and R4 pointing towards FW. Default Route on the FW towards the ISP Router R2. Static Route on R2 for the 192.1.40.0/24 network. Default Route on R3 pointing towards R2. Configure the following Loopback addresses on R1, R3 & R4: o R1 : 10.1.1.0/24 o R3 : 10.3.3.0/24 o R4 : 10.4.4.0/24 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 R3 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.23.2 255.255.255.0 No shut ! Ip route 192.1.40.0 255.255.255.0 192.1.20.10 R4 Int F 0/0 Ip address 192.1.23.3 255.255.255.0 No shut ! Int loo0 Ip add 10.3.3.3 255.255.255.0 Int F 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Int loo 0 Ip add 10.4.4.4 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 11 of 404 ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2 FW ! Ip route 0.0.0.0 0.0.0.0 192.1.40.10 Int Gig 0/0 Nameif Outside Ip add 192.1.20.10 255.255.255.0 No shut ! Int Gig 0/1 Nameif Inside Ip add 10.11.11.10 255.255.255.0 No shut ! Int Gig 0/2 Nameif DMZ Security-level 50 Ip add 192.1.40.10 255.255.255.0 No shut ! Route outside 0 0 192.1.20.2 Lab Tasks: Task 1 Configure an IPSec Tunnel to encrypt traffic from 10.3.3.0/24 on R3 (Loopback 0) to the 10.4.4.0/24 on R4 (Loopback 0) using the following parameters for IPSec: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : MD5 o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC R3 Crypto isakmp policy 10 Authentication pre-share Hash md5 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 12 of 404 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.40.4 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac ! access-list 150 permit ip 10.3.3.0 0.0.0.255 10.4.4.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.1.40.4 set transform-set t-set match address 150 ! Interface F 0/0 Crypto map I-MAP R4 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.23.3 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac ! access-list 150 permit ip 10.4.4.0 0.0.0.255 10.3.3.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.1.23.3 set transform-set t-set match address 150 ! Interface F 0/0 Crypto map I-MAP Task 2 Open the appropriate entries on the Firewall to allow the tunnel to form. ASA Access-list INF permit udp host 192.1.23.3 host 192.1.40.4 eq 500 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 13 of 404 Access-list INF permit esp host 192.1.23.3 host 192.1.40.4 ! Access-group INF in int outside ** As the Tunnel Endpoints are not getting translated, NAT-T will not be used, hence the data traffic will be transmitted in a ESP packet. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 14 of 404 Lab 2 – LAN-To-LAN Tunnel with NAT-T Lab Scenario: Configure an IPSec LAN-to-LAN Tunnel from R1 to a Router on the Internet R3. R2 is your Perimeter Router. Open the appropriate Entries in the FW ACL to allow the tunnel to form Initial Setup: Based on the previous Lab Lab Tasks: Task 1 R1 should be seen as 192.1.20.1 on the Internet. Configure a static translation on R1 to accomplish this. FW Object network R1 Host 10.11.11.1 Nat (Inside,Outside) static 192.1.20.1 Task 2 Configure an IPSec Tunnel to encrypt traffic from 10.1.1.0/24 on R1 (Loopback 0) to the 10.3.3.0/24 on R3 (Loopback 0) using the following parameters for IPSec: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : MD5 o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC R1 Crypto isakmp policy 10 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 15 of 404 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.23.3 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac ! access-list 153 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.1.23.3 set transform-set t-set match address 153 ! Interface F 0/0 Crypto map I-MAP R3 **As I am using the same ISAKMP & IPSec parameters that were used for my existing tunnel, I don’t need to re-create them. Crypto isakmp key cisco address 192.1.20.1 ! access-list 151 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 ! crypto map I-MAP 20 ipsec-isakmp set peer 192.1.20.1 set transform-set t-set match address 151 Task 3 Open the appropriate entries on the Firewall to allow the tunnel to form. ASA Access-list INF permit udp host 192.1.23.3 host 10.11.11.1 eq 500 Access-list INF permit udp host 192.1.23.3 host 10.11.11.1 eq 4500 ** As at least one of the Tunnel Endpoints (R1) is getting translated, NAT-T will be used, hence the data traffic will be transmitted in an encapsulated UDP packet. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 16 of 404 Lab 3 – Point-to-Point GRE R1 10.1.1.0/24 R3 R2 192.1.23.0/24 192.1.12.0/24 F 0/0 (.1) F 0/0 (.2) F 0/1 (.2) 10.3.3.0/24 F 0/0 (.3) Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 17 of 404 Lab Scenario: Configure a Point-to-Point GRE Tunnel from R1 to R3. R2 is your Internet Router. Initial Setup: Configure the IP Addresses based on the Diagram. Configure Default Routes on R1 and R3 pointing towards R2. Configure the following Loopback addresses on R1 & R3: o R1 : 10.1.1.1/24 and 10.1.2.1/24 o R3 : 10.3.1.1/24 and 10.3.2.1/24 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 1 Ip add 10.1.2.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.12.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.12.2 R3 Int F 0/0 Ip add 192.1.12.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.23.2 255.255.255.0 No shut Int loopback 0 Ip add 10.3.1.1 255.255.255.0 ! Int loopback 1 Ip add 10.3.2.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.23.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 18 of 404 Lab Tasks: Task 1 Configure a Point-to-Point GRE tunnel 192.168.13.0/24 as the Tunnel Network IP. between R1 and R3. Use R1 Interface Tunnel 1 Ip add 192.168.13.1 255.255.255.0 Tunnel source 192.1.12.1 Tunnel destination 192.1.23.3 R3 Interface Tunnel 1 Ip add 192.168.13.3 255.255.255.0 Tunnel source 192.1.23.3 Tunnel destination 192.1.12.1 Task 2 Configure EIGRP in AS 13 to route the internal networks (Loopbacks) on the GRE Tunnel between R1 and R3. R1 Router EIGRP 13 No auto-summary Network 192.168.13.0 Network 10.0.0.0 R3 Router EIGRP 13 No auto-summary Network 192.168.13.0 Network 10.0.0.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 19 of 404 Lab 4 – Encrypting GRE Tunnels Using IPSec Lab Scenario: Encrypt the traffic passing thru the GRE Tunnel using IPSec Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure IPSec to encrypt the traffic passing thru the GRE tunnel. Make sure the packet does not duplicate the IP addresses in the Header. Use the following parameters for the IPSec Tunnel: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : MD5 o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC R1 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.23.3 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 20 of 404 Interface Tunnel 1 Tunnel protection ipsec profile IPSEC R3 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.12.1 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set ! Interface Tunnel 1 Tunnel protection ipsec profile IPSEC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 21 of 404 Lab 5 – Configuring a Native IPSec Tunnel Interface Using Static-Virtual Tunnel Interface (S-VTI) Lab Scenario: Convert the existing GRE/IPSEC tunnel into a native IPSec tunnel by completely eliminating GRE from the Packets. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Convert the Existing GRE/IPSec tunnel to a Native IPSec tunnel by changing the Tunnel mode to IPSec. R1 Interface Tunnel 1 Tunnel mode ipsec ipv4 R3 Interface Tunnel 1 Tunnel mode ipsec ipv4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 22 of 404 CCIE Security v5 – Advanced VPNs Module 2 – Advanced VPNs Module 2 – Advanced VPNs Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 23 of 404 Lab 1 – Multipoint GRE (MGRE) Tunnel R1 10.1.1.0/24 10.1.2.0/24 F 0/0 (.1) 192.1.10.0/24 R2 R4 F 0/0 (.5) R5 192.1.40.0/24 192.1.20.0/24 10.2.1.0/24 10.2.2.0/24 F 0/0 (.2) F 0/3 (.5) F 0/1 (.5) F 0/2 (.5) F 0/0 (.4) 10.4.1.0/24 10.4.2.0/24 192.1.30.0/24 F 0/0 (.3) 10.3.1.0/24 10.3.2.0/24 R3 Lab Scenario: Configure a Multipoint GRE Tunnel between R1, R2, R3 & R4. R5 is your Internet Router. Initial Setup: Configure the IP Addresses based on the Diagram. Configure Default Routes on R1 thru R4 pointing towards R5. Configure the following Loopback addresses on R1 thru R4: o o o o R1 R2 R3 R4 : : : : 10.1.1.1/24 10.2.1.2/24 10.3.1.3/24 10.4.1.4/24 and and and and 10.1.2.1/24 10.2.2.2/24 10.3.2.3/24 10.4.2.4/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 24 of 404 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 1 Ip add 10.1.2.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.5 R3 Int loopback 0 Ip add 10.2.1.2 255.255.255.0 ! Int loopback 1 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.5 R4 Int loopback 0 Ip add 10.3.1.3 255.255.255.0 ! Int loopback 1 Ip add 10.3.2.3 255.255.255.0 ! Int F 0/0 Ip add 192.1.05.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.30.5 R5 Int loopback 0 Ip add 10.4.1.4 255.255.255.0 ! Int loopback 1 Ip add 10.4.2.4 255.255.255.0 ! Int F 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.40.5 Interface F 0/0 Ip address 192.1.10.5 No shut ! Interface F 0/1 Ip address 192.1.20.5 No shut ! Interface F 0/2 Ip address 192.1.30.5 No shut ! Interface F 0/3 Ip address 192.1.40.5 No shut 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 25 of 404 Lab Tasks: Task 1 Configure a MultiPoint GRE tunnel between R1, R2, R3 & R4. Use 192.168.1.0/24 as the Tunnel Network IP. The NHRP mapping will be done in the next Task. Use the following parameters for your MGRE Tunnel: NHRP Parameters o NHRP ID – 1234 o NHRP Authentication key – cisco Tunnel Parameters o Tunnel Authentication Key : 1234 R1 Interface Tunnel 1 Ip address 192.168.1.1 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R2 Interface Tunnel 1 Ip address 192.168.1.2 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R3 Interface Tunnel 1 Ip address 192.168.1.3 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R4 Interface Tunnel 1 Ip address 192.168.1.4 255.255.255.0 Ip nhrp network-id 1234 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 26 of 404 Ip nhrp authentication cisco Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 Task 2 Configure NHRP Mapping allowing all devices to connect to each other directly for Unicast traffic. Configure Multicast mappings in such a way that all devices use R1 as the routing hub. R1 Interface Tunnel 1 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map 192.168.1.3 192.1.30.3 Ip nhrp map 192.168.1.4 192.1.40.4 Ip nhrp map Multicast 192.1.20.2 Ip nhrp map Multicast 192.1.30.3 Ip nhrp map Multicast 192.1.40.4 R2 Interface Tunnel 1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map 192.168.1.3 192.1.30.3 Ip nhrp map 192.168.1.4 192.1.40.4 Ip nhrp map Multicast 192.1.10.1 R3 Interface Tunnel 1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map 192.168.1.4 192.1.40.4 Ip nhrp map Multicast 192.1.10.1 R4 Interface Tunnel 1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map 192.168.1.3 192.1.30.3 Ip nhrp map Multicast 192.1.10.1 Task 3 Configure EIGRP in AS 1234 to route the internal networks (Loopbacks) on the GRE Tunnel on all the MGRE Routers. Disable Split horizon on R1 to allow it propagate routes from the Spoke routers to the other spoke routers. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 27 of 404 Note: You might need to bounce the Tunnel interface to make the Routing work. Bring up the Hub router before the Spoke Routers. R1 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R2 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R3 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R4 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 28 of 404 Lab 2 – Configuring DMVPN – Phase I Lab Scenario: Configure DMVPN Phase I. The Spoke to Spoke traffic should use a Hub as a hop. Use EIGRP as the Routing Protocol. Initial Setup: Builds on the previous lab. Disable the Tunnel Interface from the previous lab R1 R2 No Interface Tunnel 1 R3 No Interface Tunnel 1 R4 No Interface Tunnel 1 No Interface Tunnel 1 Lab Tasks: Task 1 Configure a MultiPoint GRE tunnel between R1, R2, R3 & R4. Use 192.168.1.0/24 as the Tunnel Network IP. Tunnel: NHRP Parameters o NHRP ID – 1234 o NHRP Authentication key – cisco o NHS : R1 o Routing Hub: R1 [Configure the multicast mapping to accommodate routing protocols] Tunnel Parameters o Tunnel Authentication Key : 1234 R1 Interface Tunnel 1 Ip address 192.168.1.1 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp map multicast dynamic Tunnel source F 0/0 Tunnel mode gre multipoint Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 29 of 404 Tunnel key 1234 R2 Interface Tunnel 1 Ip address 192.168.1.2 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R3 Interface Tunnel 1 Ip address 192.168.1.3 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R4 Interface Tunnel 1 Ip address 192.168.1.4 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp nhs 192.168.1.1 Ip nhrp map 192.168.1.1 192.1.10.1 Ip nhrp map multicast 192.1.10.1 Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 Task 2 Configure EIGRP in AS 1234 to route the internal networks (Loopbacks) on the GRE Tunnel on all the MGRE Routers. Disable Split horizon on R1 to allow it propagate routes from the Spoke routers to the other spoke routers. R1 Interface Tunnel 1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 30 of 404 No ip split-horizon eigrp 1234 ! Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R2 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R3 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 R4 Router EIGRP 1234 No auto-summary Network 192.168.1.0 Network 10.0.0.0 Note: The default behavior of EIGRP is to change the Next-hop to itself while propagating the spoke routes to other spokes. The result is that the spokes will use the hub route as the next hop for all spoke-to-spoke traffic. This is DMVPN Phase I [Hub-n-Spoke forwarding] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 31 of 404 Lab 3 – Configuring DMVPN – Phase II Lab Scenario: Configure DMVPN Phase II. The Spoke-to-Spoke traffic should use a direct path. Use the Routing Protocol to accomplish this task. Initial Setup: Builds on the previous lab. Lab Tasks: Task 1 Disable the Hub from changing the next-hop attribute on the hub. R1 Interface Tunnel 1 No ip next-hop-self eigrp 1234 Note: Check the Routing table. The next-hop attribute for the Spoke-routes is unchanged by the hub and is directly pointing to the spoke Tunnel IP. This causes the spokes to do a NHRP resolution directly for the spoke. Although the resolution packet will go thru the hub, the actual packet will take the direct path. Use the traceroute command to verify this. This is DMVPN Phase II. In this phase, the spoke-to-spoke traffic is forwarded directly between the spokes. Phase II is accomplished by tweaking the Routing protocol behavior. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 32 of 404 Lab 4 – Configuring DMVPN – Phase III Lab Scenario: Configure DMVPN Phase III. The Spoke-to-Spoke traffic should use a direct path. Use the NHRP to accomplish this task. Initial Setup: Change the Next-hop back to Self. All routes should again have a next-hop pointing to the Hub [DMVPN Phase I] R1 Interface Tunnel 1 ip next-hop-self eigrp 1234 Lab Tasks: Task 1 Configure NHRP Redirection on the Hub such that the Hub should push down a dynamic mapping to the spokes for the spoke internal routes. Configure the spokes to accept the mapping. R1 Interface Tunnel 1 Ip nhrp redirect R2 Interface Tunnel 1 Ip nhrp shortcut R1 Interface Tunnel 1 Ip nhrp shortcut R1 Interface Tunnel 1 Ip nhrp shortcut Note: Check the Routing table. The next-hop attribute is pointing to the hun. Do a traceroute from the R2 to R4. You will notice the first trace goes thru the Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 33 of 404 hub. This is due to the routing table pointing towards the Hub. The hub detects that the spokes are both connected on the same tunnel interface, hence sends a NHRP redirect message to both of them. The NHRP redirect message contains the mapping for the destination public IP for the internal networks. The subsequent packets will be forwarded directly from spoke to spoke. If you check the routing table entry, it still points to the Hub. If you check the NHRP table, you will see an entry for the destination spoke network with the Spoke public IP. This is DMVPN Phase III. In this phase, the spoke-to-spoke traffic is forwarded directly between the spokes. Phase III is accomplished by using NHRP redirect messages to override the routing table. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 34 of 404 Lab 5 – Configuring a Dual-Hub DMVPN Lab Scenario: Configure R1 & R2 as the NHRP Hub. Initial Setup: Builds on the previous lab. Lab Tasks: Task 1 Disable the existing tunnel interface on R2. R2 No Interface Tunnel 1 Task 2 Configure a Static Tunnel between R1 and R2. R2 should be configured with a Tunnel IP address of 192.168.1.2/24 using the same Tunnel parameters as the previous lab. R2 Interface Tunnel 1 Ip address 192.168.1.2 255.255.255.0 Ip nhrp network-id 1234 Ip nhrp authentication cisco Ip nhrp map 192.168.1.1 192.1.10.10 Ip nhrp map multicast 192.1.10.1 Tunnel source F 0/0 Tunnel mode gre multipoint Tunnel key 1234 R1 Interface Tunnel1 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2 Task 2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 35 of 404 Configure R2 as another NHS in your network. Configure R3 & R4 to use R2 as the NHS Server and a Routing hub as well. R2 Interface Tunnel 1 Ip nhrp map multicast dynamic No ip split-horizon eigrp 1234 Ip nhrp redirect R3 Interface Tunnel1 Ip nhrp nhs 192.168.1.2 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2 R4 Interface Tunnel1 Ip nhrp nhs 192.168.1.2 Ip nhrp map 192.168.1.2 192.1.20.2 Ip nhrp map multicast 192.1.20.2 Note: You should now see routes from both Routing hubs. Although, it sees 2 entries, the Data path will be direct due to Phase III. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 36 of 404 Lab 6 – Encrypting the DMVPN Traffic using IPSec Lab Scenario: Configure IPSec on the Tunnel interfaces to encrypt all Tunnel traffic. Initial Setup: Builds on the previous lab. Lab Tasks: Task 1 Configure IPSec to encrypt the traffic passing thru the tunnel. Make sure the packet does not duplicate the IP addresses in the Header. Use the following parameters for the IPSec Tunnel: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : MD5 o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC R1 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 37 of 404 ! Interface Tunnel 1 Tunnel protection ipsec profile IPSEC R2 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set ! Interface Tunnel 1 Tunnel protection ipsec profile IPSEC R3 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set ! Interface Tunnel 1 Tunnel protection ipsec profile IPSEC R4 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 38 of 404 Encryption 3des ! Crypto isakmp key cisco address 0.0.0.0 ! crypto ipsec transform-set t-set esp-3des esp-sha-hmac mode transport ! crypto ipsec profile IPSEC set transform-set t-set ! Interface Tunnel 1 Tunnel protection ipsec profile IPSEC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 39 of 404 Lab 7 – Configuring GET VPN R6 R1 F 0/0 (.6) F 0/1 (.1) 10.1.1.0/24 10.1.11.0/24 192.168.16.0/24 F 0/0 (.1) 192.1.168.10.0/24 R2 R4 F 0/0 (.5) R5 192.168.20.0/24 10.1.2.0/24 10.1.22.0/24 192.168.40.0/24 F 0/3 (.5) F 0/0 (.2) F 0/1 (.2) F 0/1 (.5) F 0/2 (.5) F 0/0 (.4) 10.1.4.0/24 10.1.44.0/24 192.168.27.0/24 F 0/0 (.7) 192.168.30.0/24 F 0/0 (.3) R7 10.1.3.0/24 10.1.33.0/24 R3 Lab Scenario: Configure GET VPN to encrypt traffic between R1, R2, R3 & R4. R6 is your Key Server. R1 and R6 are located at the Head quarters. R2, R3 & R4 are remote sites connecting over a Private WAN. Initial Setup: Configure the IP Addresses based on the Diagram. Configure the following Loopback addresses on R2 thru R5: o o o o R2 R2 R3 R4 : : : : 10.1.1.1/24 10.1.2.1/24 10.1.3.1/24 10.1.4.1/24 and and and and 10.1.11.1/24 10.1.22.1/24 10.1.33.1/24 10.1.44.1/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 40 of 404 Configure EIGRP in AS 100 as the routing protocol to route all networks in the network. GETVPN requires a full routable network prior to setting up the VPN. R1 R2 Int F 0/0 Ip add 192.168.10.1 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.16.1 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.1.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.11.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.10.0 Network 192.168.16.0 Network 10.0.0.0 R3 Int F 0/0 Ip add 192.168.20.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.27.2 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.2.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.22.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.20.0 Network 192.168.27.0 Network 10.0.0.0 R4 Int F 0/0 Ip add 192.168.30.3 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.3.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.33.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.30.0 Network 10.0.0.0 R5 – Service Provider Int F 0/0 Ip add 192.168.40.4 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.4.1 255.255.255.0 ! Interface Loopback1 Ip address 10.1.44.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.40.0 Network 10.0.0.0 R6 Int F 0/0 Ip add 192.168.10.5 255.255.255.0 Int F 0/0 Ip add 192.168.16.6 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 41 of 404 No shut No shut ! Int F 0/1 Ip add 192.168.20.5 255.255.255.0 No shut ! Int F 0/2 Ip add 192.168.30.5 255.255.255.0 No shut ! Int F 0/3 Ip add 192.168.40.5 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.10.0 Network 192.168.20.0 Network 192.168.30.0 Network 192.168.40.0 R7 ! Router EIGRP 100 No auto-summary Network 192.168.16.0 Int F 0/0 Ip add 192.168.27.7 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.27.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 42 of 404 Lab Tasks: Task 1 Configure R6 as the Key Server for your GET VPN to encrypt data between R1, R2, R3 and R4. Use the following parameters for the KS. ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Pre-Shared Key : cisco [Don’t use wildcard mask] o Group : 2 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Key Server Parameters o Identity Number : 100 o Interesting Traffic : Any traffic on the 10.1.0.0/16 network. o Local Address : F 0/0 o Rekey Transport : Unicast o Rekey Key Label : GETVPN o Rekey key Encryption : 3des R6 Crypto key generate rsa modulus 1024 label GETVPN exportable [Exportable is required for Coop Server] ! crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cisco address 192.168.10.1 crypto isakmp key cisco address 192.168.20.2 crypto isakmp key cisco address 192.168.30.3 crypto isakmp key cisco address 192.168.40.4 ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 150 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 ! crypto ipsec profile G-PROF set transform-set TSET ! crypto gdoi group ABC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 43 of 404 identity number 100 server local address ipv4 192.168.16.6 sa ipsec 1 profile G-PROF match address ipv4 150 rekey transport unicast rekey authentication mypubkey rsa GETVPN rekey algorithm 3des Task 2 Configure R1, R2, R3 and R4 to use R6 as the Key Server. Use the Parameters listed for the Key server to configure the Devices. R1 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.16.6 ! crypto gdoi group ABC identity number 100 server address ipv4 192.168.16.6 ! crypto map I-MAP 10 gdoi set group ABC ! interface F 0/0 crypto map I-MAP R2 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.16.6 ! crypto gdoi group ABC identity number 100 server address ipv4 192.168.16.6 ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 44 of 404 crypto map I-MAP 10 gdoi set group ABC ! interface F 0/0 crypto map I-MAP R3 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.16.6 ! crypto gdoi group ABC identity number 100 server address ipv4 192.168.16.6 ! crypto map I-MAP 10 gdoi set group ABC ! interface F 0/0 crypto map I-MAP R4 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.16.6 ! crypto gdoi group ABC identity number 100 server address ipv4 192.168.16.6 ! crypto map I-MAP 10 gdoi set group ABC ! interface F 0/0 crypto map I-MAP! interface S0/2 crypto map I-MAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 45 of 404 Lab 8 – Configuring GET VPN Redundancy Lab Scenario: Configure a Coop server to provide fault tolerance to the Key Server. Initial Setup: Builds on the previous lab. Lab Tasks: Task 1 Export the RSA keys on R6 so that they can be imported on the Backup server [R7]. Export Parameters: o File Type: PEM o Encryption : 3DES o Encryption Key: cisco123 o Group : 2 R6 crypto key export rsa GETVPN pem terminal 3des cisco123 ---% Key name: GETVPN Usage: General Purpose Key Key data:----BEGIN PUBLIC KEY----ABCDi13330GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecT1PumBNG1fWPMm1RE /Rt/gT1WdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI pgAlPn+PldDbpbgZP4Iv9VDp7xbU+9AVVkZpnYZLjo6aGQxBvHuLPA1S31+jSgXw tDkjpNA1w48fHDAgYwIDAQAB -----END PUBLIC KEY---------BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTEDDEK-Info: DES-EDE3-CBC,4C0424B43DE3EAC5 PjSOnv50zJZWwAUA5vTRRdRffJmi5cn9yH+eTLSg1A5GilKXmT5UhKucVMzHb1ep XMaBacqt6QiJnib/MEHQAyjrbKSg5Ayvp1hTap+Vw/reOyMJovrDcCRmt3hzynz9 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 46 of 404 r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ Z3skBIKUT8CiNTmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzMjIPZ/yG8 4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2 1MLe3szgMKg6eysWYTFCXRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMUhQ OenT1u3vhjUzqxX+b/2IWYARvlY+rKahA4XkRhXwctsYB2Gs9a+dvuC+nl9JI5ys zv++hUvrxAPlxfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmdLljD2Qs+2wa8AtM q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGn/+EqlalSX5VAKfnvdnQEY5RNcN9 BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLyPS0YhjWXs3XwRz 1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdbWQ8l37XL+b6jzG sdHa5IyBbs+kIeNELJTg9W1NLNaxEUhXjTh525CEXnU= -----END RSA PRIVATE KEY----- Task 2 Import the RSA keys from R6 on R7. Import Parameters to match: o File Type: PEM o Encryption : 3DES o Encryption Key: cisco123 o Group : 2 R7 crypto key import rsa KS-KEYS pem exportable terminal cisco123 --% Enter PEM-formatted public General Purpose % End with a blank line or "quit" on a line by itself. -----BEGIN PUBLIC KEY----ABCDi13330GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCmct4j/ecT1PumBNG1fWPMm1RE /Rt/gT1WdhRDWwKmt8ftVFMU6rqjwjUqhn7hLRPortnBGS14t4UjK6IXzPLuxUbI pgAlPn+PldDbpbgZP4Iv9VDp7xbU+9AVVkZpnYZLjo6aGQxBvHuLPA1S31+jSgXw tDkjpNA1w48fHDAgYwIDAQAB -----END PUBLIC KEY----% Enter PEM-formatted encrypted private General Purpose key. % End with "quit" on a line by itself. -----BEGIN RSA PRIVATE KEY----- Proc-Type: 4,ENCRYPTED DEK-Info: DES-EDE3-CBC,4C0424B43DE3EAC5 PjSOnv50zJZWwAUA5vTRRdRffJmi5cn9yH+eTLSg1A5GilKXmT5UhKucVMzHb1ep XMaBacqt6QiJnib/MEHQAyjrbKSg5Ayvp1hTap+Vw/reOyMJovrDcCRmt3hzynz9 r/LXN/ykNKWeQvCr+YFglzMtptdEwQfhBA1P4eSMLCozP/r8Sd+oABMBIh4Im8kZ Z3skBIKUT8CiNTmKDA3B/QMe2F1bcEeaA7r0CvoMQNWG9kLwhyQnnZzMjIPZ/yG8 4RrxmpWxrL3VOnAbAXxYu/fe597JKQEcp3XnURYnNHsh4dIphemlAAegPRHLCJQR pd2an5I/Q4vAuVLaXgRRCuwe75fLUSZtk8UKAJXS3ZiOKbuABQ5QiLFS+S9Unnb2 1MLe3szgMKg6eysWYTFCXRNLauEyNhA4PMSxxLCPDeDaQr4XilB/iKMXy6ROMUhQ OenT1u3vhjUzqxX+b/2IWYARvlY+rKahA4XkRhXwctsYB2Gs9a+dvuC+nl9JI5ys Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 47 of 404 zv++hUvrxAPlxfi/YM9tVMN91Rd8kZamIPwGFHgMk7wMwqwmdLljD2Qs+2wa8AtM q+TvgQNUtqq9il0YHcRDZEiA5NWyNvcFFZKGn/+EqlalSX5VAKfnvdnQEY5RNcN9 BUpP7mLApWOBvAZz7vHC7/ZYaPeHtpabPaEvcqTXGc5mah6HLyPS0YhjWXs3XwRz 1czJ+cnBo6YXkvvTo4HefIfnnZHO+it8Y/chbny+/aVw1/fcdbWQ8l37XL+b6jzG sdHa5IyBbs+kIeNELJTg9W1NLNaxEUhXjTh525CEXnU= -----END RSA PRIVATE KEY----quit % Key pair import succeeded. Task 3 Configure R6 to point to R7 as the Backup redundancy server. R6 should be the preferred KS. Set the Local Priority to 100 on R6, R6 crypto gdoi group ABC identity number 100 server local redundancy local priority 100 peer address ipv4 192.1.27.7 Task 4 Configure R7 as the Backup Key Server for your GET VPN to encrypt data between R1, R2, R3 and R4. Use the following parameters for the KS. These are the same ones that were specified on R6. Configure redundancy pointing to R6 as the peer. Set the local priority to 50. ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Pre-Shared Key : cisco [Don’t use wildcard mask] o Group : 2 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Key Server Parameters o Identity Number : 100 o Interesting Traffic : Any traffic on the 10.1.0.0/16 network. o Local Address : F 0/0 o Rekey Transport : Unicast o Rekey Key Label : GETVPN o Rekey key Encryption : 3des R7 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 48 of 404 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cisco address 192.168.10.1 crypto isakmp key cisco address 192.168.20.2 crypto isakmp key cisco address 192.168.30.3 crypto isakmp key cisco address 192.168.40.4 ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 150 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 ! crypto ipsec profile G-PROF set transform-set TSET ! crypto gdoi group ABC identity number 100 server local address ipv4 192.168.27.7 redundancy local priority 50 peer address ipv4 192.1.16.6 sa ipsec 1 profile G-PROF match address ipv4 150 rekey transport unicast rekey authentication mypubkey rsa GETVPN rekey algorithm 3des Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 49 of 404 Lab 8 – Configuring VRF Aware GETVPN R1 10.1.1.0/24 10.1.11.0/24 F 0/0 (.1) 192.1.168.14.0/24 F 0/0 (.4) R4 R5 R3 192.168.35.0/24 192.168.45.0/24 10.1.4.0/24 x2 10.1.44.0/24 x2 F 0/1 (.5) F 0/2 (.4) F 0/1 (.4) F 0/0 (.3) F 0/0 (.5) 192.168.24.0/24 F 0/0 (.2) 10.1.2.0/24 10.1.22.0/24 R2 Lab Scenario: Configure VRF-aware IPSec LAN-TO-LAN VPNs. Initial Setup: Configure the Routers based on VPN using the following configurations: R1 R2 Int F 0/0 Ip add 192.168.14.1 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.1.1 255.255.255.0 ! Interface Loopback1 Int F 0/0 Ip add 192.168.24.2 255.255.255.0 No shut ! Interface Loopback0 Ip address 10.1.2.1 255.255.255.0 ! Interface Loopback1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 50 of 404 Ip address 10.1.11.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.14.0 Network 10.0.0.0 R3 Ip address 10.1.22.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 192.168.24.0 Network 10.0.0.0 Int F 0/0 Ip add 192.168.35.3 255.255.255.0 No shut ! ip route 0.0.0.0 0.0.0.0 192.1.35.5 R4 Vrf definition SITE-1 Vrf definition SITE-2 ! Int F 0/0 Vrf forwarding SITE-1 Ip add 192.168.14.4 255.255.255.0 No shut ! Int F 0/1 Vrf forwarding SITE-2 Ip add 192.168.24.4 255.255.255.0 No shut ! Int F 0/2 Ip add 192.168.45.4 255.255.255.0 No shut ! Interface Loopback0 Vrf forwarding SITE-1 Ip address 10.1.4.1 255.255.255.0 ! Interface Loopback1 Vrf forwarding SITE-1 Ip address 10.1.44.1 255.255.255.0 ! Interface Loopback2 Vrf forwarding SITE-2 Ip address 10.1.4.1 255.255.255.0 ! Interface Loopback3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 51 of 404 Vrf forwarding SITE-2 Ip address 10.1.44.1 255.255.255.0 ! ip route vrf SITE-1 192.168.35.3 255.255.255.255 192.168.45.5 global ! ip route vrf SITE-2 192.168.35.3 255.255.255.255 192.168.45.5 global ! ip route 192.168.14.0 255.255.255.0 F 0/0 ip route 192.168.24.0 255.255.255.0 F 0/1 ! Router EIGRP 100 No auto-summary Network 192.168.45.0 ! address-family ipv4 vrf SITE-1 autonomous-system 100 No auto-summary Network 192.168.14.0 Network 10.0.0.0 Redistribute static ! address-family ipv4 vrf SITE-2 autonomous-system 100 No auto-summary Network 192.168.24.0 Network 10.0.0.0 Redistribute static R5 Int F 0/0 Ip add 192.168.45.5 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.35.5 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.35.0 ! ip route 0.0.0.0 0.0.0.0 192.168.45.4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 52 of 404 Lab Tasks: Task 1 Configure R3 as the Key Server site SITE-1 and SITE-2 using the following parameters: SITE-1 o ISAKMP Parameters Authentication : Pre-shared Encryption : 3DES Pre-Shared Key : cisco [Don’t use wildcard mask] Group : 2 o IPSec Parameters Encryption : ESP-3DES Authentication : ESP-MD5-HMAC o Key Server Parameters Identity Number : 111 Interesting Traffic: Any traffic on the 10.1.0.0/16 network. Local Address : F 0/0 SITE-2 o ISAKMP Parameters Authentication : Pre-shared Encryption : 3DES Pre-Shared Key : cisco [Don’t use wildcard mask] Group : 2 o IPSec Parameters Encryption : ESP-3DES Authentication : ESP-MD5-HMAC o Key Server Parameters Identity Number : 222 Interesting Traffic : Any traffic on the 10.1.0.0/16 network. Local Address : F 0/0 R3 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cisco address crypto isakmp key cisco address crypto isakmp key cisco address crypto isakmp key cisco address 192.168.14.1 192.168.14.4 192.168.24.2 192.168.24.4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 53 of 404 ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 150 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 access-list 151 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 ! crypto ipsec profile G-PROF set transform-set TSET ! crypto gdoi group SITE-1 identity number 111 server local address ipv4 192.168.35.3 sa ipsec 1 profile G-PROF match address ipv4 150 ! crypto gdoi group SITE-1 identity number 222 server local address ipv4 192.168.35.3 sa ipsec 1 profile G-PROF match address ipv4 150 Task 2 Configure GETVPN for SITE-1 [R1-R4] and SITE-2 [R2-R4]. Use R3 as the Key Server. Use the Parameters listed for the Key server to configure the Devices. R1 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.35.3 ! crypto gdoi group ABC identity number 111 server address ipv4 192.168.35.3 ! crypto map I-MAP 10 gdoi set group ABC ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 54 of 404 interface F 0/0 crypto map I-MAP R2 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto isakmp key cciesec address 192.168.35.3 ! crypto gdoi group ABC identity number 111 server address ipv4 192.168.35.3 ! crypto map I-MAP 10 gdoi set group ABC ! interface F 0/0 crypto map I-MAP R4 crypto isakmp policy 10 encr 3des authentication pre-share group 2 ! crypto keyring SITE-1 vrf SITE-1 pre-shared-key address 192.168.35.3 key cisco ! crypto keyring SITE-2 vrf SITE-2 pre-shared-key address 192.168.35.3 key cisco ! crypto isakmp profile SITE-1 vrf SITE-1 match identity address 192.168.35.3 255.255.255.255 SITE-1 keyring SITE-1 ! crypto isakmp profile SITE-2 vrf SITE-1 match identity address 192.168.35.3 255.255.255.255 SITE-2 keyring SITE-2 ! Crypto gdoi group SITE-1 identity number 111 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 55 of 404 server address ipv4 192.168.35.3 ! Crypto gdoi group SITE-2 identity number 222 server address ipv4 192.168.35.3 ! crypto map SITE-1 isakmp-profile SITE-1 crypto map SITE-1 10 gdoi set group SITE-1 ! crypto map SITE-2 isakmp-profile SITE-2 crypto map SITE-2 10 gdoi set group SITE-2 ! interface F 0/0 crypto map SITE-1 ! interface F 0/0 crypto map SITE-2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 56 of 404 Lab 9 – Configuring a Router as a CA Server R1 192.168.23.0/24 192.168.12.0/24 10.1.1.0/24 R3 R2 F 0/0 (.1) F 0/1 (.2) F 0/0 (.2) 10.3.3.0/24 F 0/0 (.3) Lab Scenario: Configuring R2 as a CA Server. Configuring a VPN Tunnel to encrypt traffic between R1 & R3 using RSA-Signatures. Also, to encrypt traffic from R2 to R3. Initial Setup: Configure the IP Addresses based on the Diagram. Configure the following Loopback addresses on R1 thru R3. o R1 : 10.1.1.1/24 o R2 : 10.2.2.2/24 o R3 : 10.3.3.3/24 Configure EIGRP in AS 100 as the routing protocol to route all networks in the network. R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 192.168.12.1 255.255.255.0 Clock rate 128000 No shut Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.168.12.2 255.255.255.0 No shut ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 57 of 404 ! Router EIGRP 100 No auto-summary Network 192.168.12.0 Network 10.0.0.0 Int F 0/1 Ip add 192.168.23.2 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.12.0 Network 192.168.23.0 Network 10.0.0.0 R3 Int loopback 0 Ip add 10.3.3.3 255.255.255.0 ! Int F 0/0 Ip add 192.168.23.3 255.255.255.0 No shut ! Router EIGRP 100 No auto-summary Network 192.168.23.0 Network 10.0.0.0 Lab Tasks: Task 1 Assign R2 a domain name of ABC.com. Also set the timezone and clock to the current timezone and time. Configure R2 to be the CA Server to automatically grant certificates using the following parameters: RSA Key Size: 512 Bits Key Label: IOS-CA Any Passphrase: CCIESEC3 Issuer Name: CN=IOS-CA.ABC.com L=ND C=IN R2 Ip domain-name ABC.com ! clock timezone IST 5 30 ! clock set 12:00:00 1 May 2009 ! crypto key generate rsa general-keys label IOS-CA ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 58 of 404 ip http server ! Crypto pki server IOS-CA database url nvram: issuer-name CN=IOS-CA.NM.com L=ND C=IN grant auto no shut *** At this point R2 has a Root Certificate that it will use to Sign and Verify all certificates that it issues. Task 2 Assign R1 and R3 a domain name of ABC.com. Also set the timezone and clock to the current timezone and time. R1 Ip domain-name ABC.com ! clock timezone IST 5 30 ! clock set 12:00:00 1 May 2009 R3 Ip domain-name ABC.com ! clock timezone IST 5 30 ! clock set 12:00:00 1 May 2009 Task 3 Generate 512 Bit RSA keys on R1 and R3. Configure R1 & R3 to request a certificate from R2, the IOS-based CA Server. Use CISCO123 as the recovery password. Disable CRL checking. R1 crypto key generate rsa ! crypto ca trustpoint IOS-CA enrollment url revocation-check none ! crypto ca authenticate IOS-CA ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 59 of 404 crypto ca enroll IOS-CA R3 crypto key generate rsa ! crypto ca trustpoint IOS-CA enrollment url revocation-check none ! crypto ca authenticate IOS-CA ! crypto ca enroll IOS-CA Task 4 Configure an IPSec Tunnel to encrypt traffic between 10.1.1.0 and 10.3.3.0 networks. Use the following parameters for the tunnel: Authentication type = RSA-SIG Hash = MD5 Diffie-Hellman = 2 Encryption = 3DES IPSec Encryption = ESP-3DES IPSec Authentication = ESP-MD5-HMAC R1 Crypto isakmp pol 10 group 2 hash md5 encr 3des ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 155 permit ip 10.1.1.0 0.0.0.255 10.3.3.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.168.23.3 set transform-set TSET match address 155 ! int F 0/0 crypto map I-MAP R3 Crypto isakmp pol 10 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 60 of 404 group 2 hash md5 encr 3des ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 155 permit ip 10.3.3.0 0.0.0.255 10.1.1.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.168.12.1 set transform-set TSET match address 155 ! int F 0/0 crypto map I-MAP Task 5 Configure an IPSec Tunnel to encrypt traffic between 10.2.2.0 and 10.3.3.0 networks. Use the following parameters for the tunnel: Authentication type = RSA-SIG Hash = MD5 Diffie-Hellman = 2 Encryption = 3DES IPSec Encryption = ESP-3DES IPSec Authentication = ESP-MD5-HMAC Task 6 As the previous task requires the CA Server to also participate in the Data encryption, it requires to generate a separate key pair for that and request a Identity certificate from itself. So Generate a separate RSA key pair and request a certificate before configuring the IPSec Tunnel. R2 crypto key generate rsa ! crypto ca trustpoint IOS-CA enrollment url revocation-check none ! crypto ca authenticate IOS-CA ! crypto ca enroll IOS-CA ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 61 of 404 Crypto isakmp pol 10 group 2 hash md5 encr 3des ! crypto ipsec transform-set TSET esp-3des esp-md5-hmac ! access-list 155 permit ip 10.2.2.0 0.0.0.255 10.3.3.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.168.23.3 set transform-set TSET match address 155 ! int F 0/1 crypto map I-MAP R3 ! As we are using the same set of parameters for ISAKMP and IPSec that ! were used in the previous tunnel, I don’t need to redefine them. ! access-list 156 permit ip 10.3.3.0 0.0.0.255 10.2.2.0 0.0.0.255 ! crypto map I-MAP 20 ipsec-isakmp set peer 192.168.23.2 set transform-set TSET match address 156 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 62 of 404 Lab 9 – EZVPN – Client Mode R6 F 0/0 (.6) 10.16.16.0/24 F 0/0 (.1) R1 S 0/0 (.1) 192.1.15.0/24 R2 192.1.25.0/24 S 0/0 (.2) S 0/0 (.5) R5 S 0/1 (.5) R4 192.1.45.0/24 S 0/3 (.5) S 0/0 (.4) S 0/2 (.5) 192.1.35.0/24 S 0/0 (.3) R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 63 of 404 Lab Scenario: Configure R1 as an EZVPN Server for your Network. Your Internal network (10.16.16.0/24) should be accessible to clients thru EZVPN. R5 is your Internet Router. Configure R2 as the EZVPN Client in Client Mode. Initial Setup: Configure the IP Addresses based on the Diagram. Configure Default Routes on R1 thru R3 pointing towards R5. Configure a Static route for the 192.1.12.0/24 network on R4 with a next-hop pointing to R5. We will use this router in a later lab for a client-side Virtual Interface setup. Configure a default route on R6 pointing towards R1. Configure the following Loopback addresses on R1 thru R4: o o o o R1 R2 R3 R4 : : : : 10.1.1.1/24 10.2.2.2/24 10.3.3.3/24 10.4.4.4/24 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.16.16.1 255.255.255.0 No shut ! Int S 0/0 Ip add 192.1.15.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.15.5 R3 Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int S 0/0 Ip add 192.1.25.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.25.5 R4 Int loopback 0 Ip add 10.3.1.1 255.255.255.0 ! Int S 0/0 Ip add 192.1.35.3 255.255.255.0 No shut Int loopback 0 Ip add 10.4.1.1 255.255.255.0 ! Int S 0/0 Ip add 192.1.45.4 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 64 of 404 ! Ip route 0.0.0.0 0.0.0.0 192.1.35.5 R5 ! Ip route 192.1.12.0 255.255.255.0 192.1.45.5 R6 Interface S 0/0 Ip address 192.1.15.5 Clock rate 128000 No shut ! Interface S 0/1 Ip address 192.1.25.5 Clock rate 128000 No shut ! Interface S 0/2 Ip address 192.1.35.5 Clock rate 128000 No shut ! Interface S 0/3 Ip address 192.1.35.5 Clock rate 128000 No shut Interface F 0/0 Ip address 10.16.16.6 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.16.16.6 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Lab Tasks: Task 1 We will configure R1 as an EZVPN Server. Start by configuring the ISAKMP policy parameters that will be pushed down to the clients based on the following: ISAKMP Parameters o Authentication : Pre-shared o Group : 2 (**Minimum requirement for EZVPN) o Encryption : 3DES R1 Crypto isakmp policy 10 Authentication pre-share hash sha group 2 encryption 3des Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 65 of 404 Task 2 Configure the IPSec Transform-set parameters based on the following: IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC R1 crypto ipsec transform-set t-set esp-3des esp-md5-hmac Task 3 Configure a Pool called EZP. This pool will be assigned to EZVPN clients. Use 192.168.11.201 thru 192.168.11.225 as the pool addresses. R1 Ip local pool EZP 192.168.11.201 192.168.11.225 Task 4 We will configuring R2 as a EZVPN client. Configure a local username R2 with a password of cisco123 for Extended Authentication. Configure an ISAKMP Client Group called EZC with the following parameters: Key = cisco Dns address = 192.1.10.49 WINS address = 192.1.10.50 Pool = EZP R1 Username R2 password cisco123 ! Crypto isakmp client configuration group EZC Key cisco Dns 192.1.10.49 Wins 192.1.10.50 Pool EZP Task 5 Configure an IPSec Profile and attach the transform-set created in one of the previous set to it. This profile will be applied to virtual-template interface. R1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 66 of 404 Crypto ipsec profile EZPROF Set transform-set t-set Task 6 Enable AAA on the router. Configure Local Authentication and Network Authorization lists that will be used later on in the ISAKMP Profiles to specify authentication and authorization to be done based on Local Databases. R1 Aaa new-model ! aaa authorization network l-author local aaa authentication login l-authen local Task 7 Configure a Virtual-Template. Use the Tunnel type for this virtual-template interface. Use any Interface for the acquiring the IP Address for the Template interface. This interface should be a template for a Native Tunnel Interface. The tunnel should encrypt using the IPSec profile that was created in one of the previous steps R1 interface Virtual-Template1 type tunnel ip unnumbered F0/0 tunnel mode ipsec ipv4 tunnel protection ipsec profile EZPROF Task 8 Configure an ISAKMP Profile to link the above settings. Configure Extended Authentication and Authorization to be done based on the Local Database. R1 should respond to client requests for IP Address configurations. R1 crypto isakmp profile EZC match identity group EZC client authentication list L-AUTHEN isakmp authorization list L-AUTHOR client configuration address respond virtual-template 1 Task 9 Configure R2 as a EZVPN client using the following parameters: Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 67 of 404   Mode : Client. Peer Address : 192.1.15.1 Connect : Auto Group Name : EZC Key : cisco Traffic : Network 10.2.2.0/24 (Loopback0) going outside of the S 0/0 interface. R2 Crypto ipsec client ezvpn EZ Group EZC key cisco Peer 192.1.15.1 Connect auto Mode client ! Int loopback 0 crypto ipsec client ezvpn EZ inside ! Int S 0/0 Crypto ipsec client ezvpn EZ outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 68 of 404 Lab 10 – EZVPN – Network-Extension Mode Lab Scenario: Configure R1 to allow R3 to connect in as a EZVPN Client. The 10.16.16.0/24 network should have access to the 10.3.3.0/24 because of which you have to configure R3 as a client in Network Extension mode. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 R3 will be configured as a client in Network Extension mode so that the 10.16.16.0/24 network can access the 10.3.3.0/24 network. R3 should only encrypt traffic that is destined to the 10.16.16.0/24 network. Configure an Split-tunnel ACL on R1 to accomplish this. Use the same Virtual-template for the D-VTI. Do not do any extended authentication for this client. Configure a separate ISAKMP group and Profile for this. R1 Access-list 101 permit ip 10.16.16.0 0.0.0.255 any ! crypto isakmp client configuration group R3 Key cisco Acl 101 ! Crypto isakmp profile R3 Match identity group R3 Isakmp authorization list L-AUTHOR Client configuration address respond Virtual-template 1 Task 2 Configure R3 as a EZVPN client using the following parameters: Mode : Network Extension Mode Peer Address : 192.1.15.1 Connect : Auto Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 69 of 404 Group Name : R3 Key : cisco Traffic : Network 10.3.3.0/24 (Loopback0) going outside of the S 0/0 interface. R3 Crypto ipsec client ezvpn EZ Group EZC key cisco Peer 192.1.15.1 Connect auto Mode Network-extension ! Int loopback 0 crypto ipsec client ezvpn EZ inside ! Int S 0/0 Crypto ipsec client ezvpn EZ outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 70 of 404 CCIE Security v5 – Advanced VPNs Module 3 – Configuring VPNS Using IKEv2 Module 3 – Configuring VPNs Using IKEv2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 71 of 404 Lab 1 – Site-To-Site IPSec VPN Using IKEv2 – Crypto Maps R1 10.1.1.0/24 10.1.2.0/24 F 0/0 (.1) 192.1.10.0/24 R2 R4 F 0/0 (.5) R5 192.1.40.0/24 192.1.20.0/24 10.2.1.0/24 10.2.2.0/24 F 0/0 (.2) F 0/3 (.5) F 0/1 (.5) F 0/2 (.5) F 0/0 (.4) 10.4.1.0/24 10.4.2.0/24 192.1.30.0/24 F 0/0 (.3) 10.3.1.0/24 10.3.2.0/24 R3 Lab Scenario: Configure an IPSec tunnel to encrypt traffic from the R1 to R2 to encrypt traffic from the 10.1.0.0/16 network to the 10.2.0.0/16 using IKEv2. Use Crypto Maps for this Lab. Initial Setup: Configure the IP Addresses based on the Diagram. Configure Default Routes on R1 thru R4 pointing towards R5. Configure the following Loopback addresses on R1 thru R4: o R1 : 10.1.1.1/24 and 10.1.2.1/24 o R2 : 10.2.1.2/24 and 10.2.2.2/24 o R3 : 10.3.1.3/24 and 10.3.2.3/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 72 of 404 o R4 : 10.4.1.4/24 and 10.4.2.4/24 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 1 Ip add 10.1.2.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.5 R3 Int loopback 0 Ip add 10.2.1.2 255.255.255.0 ! Int loopback 1 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.5 R4 Int loopback 0 Ip add 10.3.1.3 255.255.255.0 ! Int loopback 1 Ip add 10.3.2.3 255.255.255.0 ! Int F 0/0 Ip add 192.1.05.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.30.5 R5 Int loopback 0 Ip add 10.4.1.4 255.255.255.0 ! Int loopback 1 Ip add 10.4.2.4 255.255.255.0 ! Int F 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.40.5 Interface F 0/0 Ip address 192.1.10.5 No shut ! Interface F 0/1 Ip address 192.1.20.5 No shut ! Interface F 0/2 Ip address 192.1.30.5 No shut ! Interface F 0/3 Ip address 192.1.40.5 No shut 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 73 of 404 Lab Tasks: Task 1 Configure a IPSec Tunnel to encrypt traffic from 10.1.0.0/16 on R1 (Loopback 0 & Loopback 1) to the 10.2.0.0/16 on R2 (Loopback 0 & Loopback 1). Task 2 Use the following Parameters for the Tunnel between R1 and R2: IKEv2 Proposal Parameters o Integrity : SHA1 o Encryption : 3DES o Group : 2 o Authentication : Pre-share o Pre-Shared Key (R1): cisco1 o Pre-Shared Key (R2): cisco2 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC R1 crypto ikev2 proposal PROP1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL1 proposal PROP1 ! crypto ikev2 keyring KR_R2 peer R2 address 192.1.20.2 pre-shared local cisco1 pre-shared remote cisco2 ! crypto ikev2 profile PROF1 match identity remote address 192.1.20.2 255.255.255.255 authentication local pre-share authentication remote pre-share keyring local KR_R2 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! Copyrights KBITS Inc 2006-2020 Website: ; Email: khaw Page 74 of 404 access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 ! crypto map ABC 10 ipsec-isakmp match address 101 set peer 192.1.20.2 set transform-set ABC set ikev2-profile PROF1 ! int F 0/0 crypto map ABC R2 crypto ikev2 proposal PROP1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL1 proposal PROP1 ! crypto ikev2 keyring KR_R1 peer R1 address 192.1.10.1 pre-shared local cisco2 pre-shared remote cisco1 ! crypto ikev2 profile PROF1 match identity remote address 192.1.10.1 255.255.255.255 authentication local pre-share authentication remote pre-share keyring local KR_R1 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! access-list 101 permit ip 10.1.0.0 0.0.255.255 10.1.0.0 0.0.255.255 ! crypto map ABC 10 ipsec-isakmp match address 101 set peer 192.1.10.1 set transform-set ABC set ikev2-profile PROF1 ! int F 0/0 crypto map ABC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 75 of 404 Lab 2 – Site-To-Site IPSec VPN Using IKEv2 – S–VTI Lab Scenario: Configure an IPSec tunnel to encrypt traffic from the R3 to R4 to encrypt traffic from the 10.3.0.0/16 network to the 10.4.0.0/16 using IKEv2. Use Native IPSec Tunnel for this Lab. Initial Setup: Based on the previous Lab Lab Objectives: Task 1 Configure a Native IPSec Tunnel to Connect R3 to R4. Use the following Parameters for the Tunnel between R3 and R4: IKEv2 Proposal Parameters o Integrity : SHA1 o Encryption : 3DES o Group : 2 o Authentication : Pre-share o Pre-Shared Key (R3): cisco3 o Pre-Shared Key (R4): cisco4 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Tunnel Parameters o Address : 192.168.34.0/24 o Tunnel Protocol : IPSec R3 crypto ikev2 proposal PROP1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL1 proposal PROP1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 76 of 404 ! crypto ikev2 keyring KR_R4 peer R4 address 192.1.40.4 pre-shared local cisco3 pre-shared remote cisco4 ! crypto ikev2 profile PROF1 match identity remote address 192.1.40.4 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_R4 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF1 ! int tunnel 1 ip add 192.168.34.3 255.255.255.0 tunnel source 192.1.30.3 tunnel destination 192.1.40.4 tunnel mode ipsec ipv4 tunnel protection ipsec profile ABC R4 crypto ikev2 proposal PROP1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL1 proposal PROP1 ! crypto ikev2 keyring KR_R3 peer R3 address 192.1.30.3 pre-shared local cisco4 pre-shared remote cisco3 ! crypto ikev2 profile PROF1 match identity remote address 192.1.30.3 255.255.255.255 authentication remote pre-share authentication local pre-share Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 77 of 404 keyring local KR_R3 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF1 ! int tunnel 1 ip add 192.168.34.4 255.255.255.0 tunnel source 192.1.40.4 tunnel destination 192.1.30.3 tunnel mode ipsec ipv4 tunnel protection ipsec profile ABC Task 2 Configure EIGRP in AS 23 between R2 & R3 on the Tunnel Interface. Injecct the Loopback Networks into EIGRP. R2 router eigrp 34 network 10.0.0.0 network 192.168.34.0 R3 router eigrp 34 network 10.0.0.0 network 192.168.34.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 78 of 404 CCIE Security v5 – Advanced VPNs Module 4 – Configuring Flex VPNS Module 4 – Configuring Flex VPNs Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 79 of 404 Lab 1 – Site-To-Site IPSec VPN Using Flex VPN R1 10.1.1.0/24 10.1.2.0/24 F 0/0 (.1) 192.1.10.0/24 R2 R6 F 0/0 (.6) F 0/0 (.2) F 0/1 (.6) F 0/2 (.6) 192.1.30.0/24 F 0/0 (.3) R5 192.1.50.0/24 192.1.20.0/24 10.2.1.0/24 10.2.2.0/24 F 1/0 (.6) F 0/0 (.5) F 0/3 (.6) 10.5.1.0/24 10.5.2.0/24 192.1.40.0/24 F 0/0 (.4) 10.3.1.0/24 10.3.2.0/24 10.4.1.0/24 10.4.2.0/24 R3 R4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 80 of 404 Lab Scenario: Configure a Site-to-Site IPSec Flex VPN between R1 & R6. Initial Setup: Configure the IP Addresses based on the Diagram. Configure Default Routes on R1, R2, R3, R4 & R6 towards R5. R5 is acting as the Internet. Configure the following Loopback addresses on R1,R2, R3, R4 & R6: o o o o o R1 R2 R3 R4 R5 : : : : : 10.1.1.1/24 10.2.1.2/24 10.3.1.3/24 10.4.1.4/24 10.5.1.5/24 & & & & & 10.1.2.1/24 10.2.2.2/24 10.3.2.3/24 10.4.2.4/24 10.5.2.5/24 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 0 Ip add 10.1.2.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.10.6 R3 Int loopback 0 Ip add 10.2.1.2 255.255.255.0 ! Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.6 R4 Int loopback 0 Ip add 10.3.1.3 255.255.255.0 ! Int loopback 0 Ip add 10.3.2.3 255.255.255.0 ! Int F 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Int loopback 0 Ip add 10.4.1.4 255.255.255.0 ! Int loopback 0 Ip add 10.4.2.4 255.255.255.0 ! Int F 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 81 of 404 Ip route 0.0.0.0 0.0.0.0 192.1.30.6 R5 Int loopback 0 Ip add 10.5.1.2 255.255.255.0 ! Int loopback 0 Ip add 10.5.2.5 255.255.255.0 ! Int F 0/0 Ip add 192.1.50.5 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.50.6 Ip route 0.0.0.0 0.0.0.0 192.1.40.6 R6 Interface F 0/0 Ip address 192.1.10.6 255.255.255.0 No shut ! Interface F 0/1 Ip address 192.1.20.6 255.255.255.0 No shut ! Interface F 0/2 Ip address 192.1.30.6 255.255.255.0 No shut ! Interface F 0/3 Ip address 192.1.40.6 255.255.255.0 No shut ! Interface F 1/0 Ip addres 192.1.50.6 255.255.255.0 255.255.255.0 No shut Lab Tasks: Task 1 Configure a Site-to-Site Flex VPN to encrypt traffic from 10.1.X.0/24 networks on R1 (Loopback 0 & Loopback 1) to the 10.5.X.0/24 on R5 (Loopback 0 & Loopback 1). Task 2 Use the following Parameters for the Tunnel between R1 and R5: IKEv2 Proposal Parameters o Integrity : SHA1 o Encryption : 3DES o Group : 2 o Authentication : Pre-share o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Tunnel IP Address: o IP Address for Virtual-template on R1 : 192.168.1.1/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 82 of 404 o Tunnel Interface on R5 : 192.168.1.5/24 R1 int loo1 ip add 192.168.1.1 255.255.255.0 ! int virtual-template 1 type tunnel ip unnumbered Lo11 tunnel source 192.1.10.1 tunnel mode ipsec ipv4 ! crypto ikev2 proposal PROP_1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL_1 proposal PROP_1 ! crypto ikev2 keyring KR_R5 peer R5 address 192.1.50.5 pre-shared local cisco pre-shared remote cisco ! crypto ikev2 profile PROF_1 match identity remote address 192.1.50.5 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_R5 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF_1 ! int virtual-template 1 type tunnel tunnel protection ipsec profile ABC ! crypto ikev2 profile PROF_1 virtual-template 1 ! router eigrp 100 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 83 of 404 network 10.0.0.0 network 192.168.1.0 R5 crypto ikev2 proposal PROP_1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL_1 proposal PROP_1 ! crypto ikev2 keyring KR_R1 peer R1 address 192.1.10.1 pre-shared local cisco pre-shared remote cisco ! crypto ikev2 profile PROF_1 match identity remote address 192.1.10.1

255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_R1 ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF_1 ! int tunnel 1 ip add 192.168.1.5 255.255.255.0 tunnel source 192.1.50.5 tunnel destination 192.1.10.1 tunnel mode ipsec ipv4 tunnel protection ipsec profile ABC ! router eigrp 100 network 10.0.0.0 network 192.168.1.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 84 of 404 Lab 2 – Spoke-To-Spoke IPSec VPN Using Flex VPN Lab Scenario: Configure a Spoke-to-Spoke Tunnel between R1, R2 & R3 Using Flex VPN. Initial Setup: Based on the previous Lab Lab Objectives: Task 1 Configure a Spoke-to-Spoke IPSec tunnel using Flex VPN to encrypt traffic between R1, R2 & R3. Use the following parameters: IKEv2 Proposal Parameters o Integrity : SHA1 o Encryption : 3DES o Group : 2 o Authentication : Pre-share o Pre-Shared Key : cisco100 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Tunnel Parameters o Pool : FLEX – 192.168.2.101 192.168.2.200 o NHRP Network ID : 100 o Tunnel Interface # : 2 o Virtual-Template # : 2 R1 ip local pool FLEX 192.168.2.2 192.168.2.254 ! Interface loopback 2 Ip address 192.168.2.1 255.255.255.0 ! crypto ikev2 authorization policy default pool FLEX route set interface Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 85 of 404 ! crypto ikev2 keyring KR_ALL peer ALL address 0.0.0.0 0.0.0.0 pre-shared-key cisco100 ! aaa new-model aaa authorization network default local ! interface Virtual-Template2 type tunnel ip unnumbered Loopback2 ip nhrp network-id 100 ip nhrp redirect ! crypto ikev2 profile PROF_R2R3 match identity remote address 192.1.20.2 255.255.255.255 match identity remote address 192.1.30.3 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_ALL aaa authorization group override psk list default default virtual-template 2 ! crypto ipsec profile R2R3 set transform-set ABC set ikev2-profile PROF_R2R3 ! router eigrp 100 redistribute static network 192.168.2.0 ! interface Virtual-Template2 type tunnel tunnel protection ipsec profile R2R3 no ip next-hop-self eigrp 100 R2 crypto ikev2 proposal PROP_1 encryption 3des integrity sha1 group 2 ! crypto ikev2 policy POL_1 proposal PROP_1 ! crypto ikev2 keyring KR_ALL Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 86 of 404 peer ALL address 0.0.0.0 0.0.0.0 pre-shared-key cisco100 ! aaa new-model aaa authorization network default local ! crypto ikev2 authorization policy default route set interface ! interface Tunnel2 ip address negotiated ip nhrp network-id 100 ip nhrp shortcut ip nhrp redirect tunnel source 192.1.20.2 tunnel destination 192.1.10.1 ! crypto ikev2 profile PROF_1 match identity remote address 0.0.0.0 authentication remote pre-share authentication local pre-share keyring local KR_ALL aaa authorization group override psk list default default ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF_1 ! interface Tunnel2 tunnel protection ipsec profile ABC ! router eigrp 100 no auto-summary network 10.0.0.0 network 192.168.2.0 R3 crypto ikev2 proposal PROP_1 encryption 3des integrity sha1 group 2 ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 87 of 404 crypto ikev2 policy POL_1 proposal PROP_1 ! crypto ikev2 keyring KR_ALL peer ALL address 0.0.0.0 0.0.0.0 pre-shared-key cisco100 ! aaa new-model aaa authorization network default local ! crypto ikev2 authorization policy default route set interface ! interface Tunnel2 ip address negotiated ip nhrp network-id 100 ip nhrp shortcut ip nhrp redirect tunnel source 192.1.30.3 tunnel destination 192.1.10.1 ! crypto ikev2 profile PROF_1 match identity remote address 0.0.0.0 authentication remote pre-share authentication local pre-share keyring local KR_ALL aaa authorization group override psk list default default ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF_1 ! interface Tunnel2 tunnel protection ipsec profile ABC ! router eigrp 100 no auto-summary network 10.0.0.0 network 192.168.2.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 88 of 404 Lab 3 – Server – Client IPSec Flex VPN Lab Scenario: Configure a Server Client IPSec Flex VPN between R1 and R4. R1 is the Server and R4 is the Client. Initial Setup: Based on the previous Lab Lab Objectives: Task 1 Configure a Server – Client IPSec tunnel using Flex VPN to encrypt traffic between R1 & R4. Use the following parameters: IKEv2 Proposal Parameters o Integrity : SHA1 o Encryption : 3DES o Group : 2 o Authentication : Pre-share o Pre-Shared Key : cisco14 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-MD5-HMAC Tunnel Parameters o Pool : FLEX (Previously Created) o Tunnel Interface # : 3 o Virtual-Template # : 3 R1 int virtual-template 3 type tunnel ip unnumbered Lo2 tunnel source 192.1.10.1 tunnel mode ipsec ipv4 ! access-list 1 permit 10.1.1.0 0.0.0.255 access-list 1 permit 10.1.2.0 0.0.0.255 ! crypto ikev2 keyring KR_CLIENTS Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 89 of 404 peer Clients address 0.0.0.0 pre-shared cisco14 ! crypto ikev2 authorization policy default pool FLEX route set interface route set access-list 1 ! crypto ikev2 profile PROF_CLIENTS match identity remote address 192.1.40.4 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_CLIENTS aaa authorization group over psk list default default virtual-template 3 ! Crypto ipsec profile CLIENTS set transform-set ABC set ikev2-profile PROF_CLIENTS ! int virtual-template 3 type tunnel tunnel protection ipsec profile CLIENTS R4 aaa new-model aaa authorization network default local ! access-list 1 permit 10.4.1.0 0.0.0.255 access-list 1 permit 10.4.2.0 0.0.0.255 ! crypto ikev2 proposal PROP_1 integrity sha1 group 2 encryption 3des ! crypto ikev2 policy POL_1 proposal PROP_1 ! crypto ikev2 keyring KR_R1 peer R1 address 192.1.10.1 pre-shared cisco14 ! crypto ikev2 authorization policy default Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 90 of 404 route set access-list 1 route set interface ! crypto ikev2 profile PROF_1 match identity remote address 192.1.10.1 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR_R1 aaa authorization group override psk list default default ! crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC set ikev2-profile PROF_1 ! int tunnel 1 ip add negotiated tunnel source 192.1.40.4 tunnel destination dynamic tunnel mode ipsec ipv4 tunnel protection ipsec profile ABC ! crypto ikev2 client flexvpn flex peer 1 192.1.10.1 connect auto client connect Tunnel1 ! router eigrp 100 net 192.168.2.0 net 10.0.0.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 91 of 404 CCIE Security v5 – Configuring Router & Switch Security Features Module 1 – Control Plane Management Module 1 – Control Plane Management Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 92 of 404 Lab 1 – Configuring Control Plane Policing SW1 R1 (.15) F 0/0 (.1) SW2 (.20) 192.1.10.0/24 VLAN 10 F 0/0 (.4) F 0/0 (.2) R4 R2 F 0/1 (.2) 192.1.23.0/24 VLAN 23 F 0/0 (.3) R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 93 of 404 Lab Scenario: Configure the Router for Control Plane Policing for Telnet Traffic. The lab is based on the following physical setup: o R1 – R6 F 0/0 are connected to SW1 ports F0/1 – respectively. For Example, F0/0 on R1 is connected to SW1 F0/0 on R2 is connected to SW1 F 0/2 ….. o R1 – R6 F 0/1 are connected to SW2 ports F0/1 – respectively. For Example, F0/1 on R1 is connected to SW2 F0/1 on R2 is connected to SW2 F 0/2 ….. o Switches are trunked over on ports F0/20 & F0/21 F 0/6 F0/1 , F 0/6 F0/1 , Initial Setup: Configure the IP Addresses on the Routers & SW based on the Diagram. Configure the 2 switches to trunk using dot1q. Configure SW1 as the VTP Server in domain cisco. Configure SW2 as the VTP Client in domain cisco. Configure all the VLANs required on SW1. Assign the devices to the appropriate VLANs. Run EIGRP in AS 100 on the Routers and SW to have complete routing in the network. R1 R2 Int F 0/0 Ip add 192.1.10.1 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.10.0 R3 Int F 0/0 Ip add 192.1.10.2 255.255.255.0 No shut ! Int F 0/0 Ip add 192.1.23.2 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.10.0 Network 192.1.23.0 R4 Int F 0/0 Int F 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 94 of 404 Ip add 192.1.23.3 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.23.0 R5 Ip add 192.1.10.4 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.10.0 Int F 0/0 Ip add 192.1.10.5 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.10.0 SW1 Interface range F 0/20 – 21 Swithcport trunk encapsulation dot1q Switchport mode trunk ! Vtp mode server Vtp domain cisco ! Vlan 10 Vlan 23 ! Interface range F 0/1 , F 0/2, F 0/4 Switchport mode access Switchport access vlan 10 ! Interface range F 0/3 Switchport mode access Switchport access vlan 23 ! Ip routing ! Interface VLAN 10 Ip address 192.1.10.15 255.255.255.0 SW2 Interface range F 0/20 – 21 Swithcport trunk encapsulation dot1q Switchport mode trunk ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 95 of 404 Vtp mode client Vtp domain cisco ! Interface F 0/2 Switchport mode access Switchport access vlan 23 ! Ip routing ! Interface VLAN 10 Ip address 192.1.10.20 255.255.255. Lab Tasks: Task 1 R3 has been configured to allow telnet access for management purposes. Using Control Plane Policing, control the rate of Telnet traffic to 64000 bps. R3 access-list 111 permit tcp any any eq 23 ! class-map TELNET match access-group 101 ! policy-map CP-Police class TELNET police 64000 ! control-plane service-policy input CP-Police Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 96 of 404 Lab 2 – Configuring Control Plane Protection for Port Filtering Lab Scenario: Configure a Router for Control Plane Port-Filtering. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R3 with a port-filter to drop all traffic destined to a custom udp port 11223. It should also drop traffic to all unused port numbers. R3 class-map type port-filter match-any CM-PF match port udp 11223 match closed-ports ! policy-map type port-filter PM-PF class CM-PF drop ! control-plane host service-policy type port-filter input PM-PF Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 97 of 404 CCIE Security v5 – Configuring Router & Switch Security Features Module 2 – Configuring Router Security Features Module 2 – Configuring Security Features Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 98 of 404 Router Lab 1 – Configuring Anti-Spoofing ACL & the RPF Feature SW1 R1 (.15) F 0/0 (.1) SW2 (.20) 192.1.10.0/24 VLAN 10 F 0/0 (.4) F 0/0 (.2) R4 R2 F 0/1 (.2) 192.1.23.0/24 VLAN 23 F 0/0 (.3) R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 99 of 404 Lab Scenario: Configure R2 to block all RFC 1918 addresses coming in from R3. R2 should also implement strict RPF to verify that the source is coming in from the valid interface. Log all packets that fail the RPF check. Initial Setup: Based on the previous Lab Lab Task: Task 1 Block any RFC 1918 address coming into R2 from R3. R2 Access-list 121 deny ip 10.0.0.0 0.255.255.255 any Access-list 121 deny ip 172.16.0.0 0.15.255.255 any Access-list 121 deny ip 192.168.0.0 0.0.255.255 any Access-list 121 permit ip any any ! Interface F 0/1 Ip access-group 121 in Task 2 Use Strict RPF to prevent IP spoofing using network addresses from the internal networks. The route could use the default gateway to check for the source address. Also make sure all packets that are failing the RPF check get logged. R2 Access-list 131 deny ip any any log ! Interface F 0/1 ip verify unicast source reachable-via rx allow-default 131 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 100 of 404 Lab 2 – Configuring NTP with Authentication Lab Scenario: Configure a Router as Clock Provider using NTP. Configure a Router to acquire the time from a remote Time source using NTP. Authenticate the NTP Relationship. Initial Setup: Based on the previous Lab Lab Task: Lab Objectives: Task 1 Configure R1 as a NTP Master with a stratum of 2. R1 is in New Delhi (+5:30). Configure the appropriate Time Zone setting. Set the Router clock based on the current date and time. R1 clock timezone IST 5 30 ! Do clock set hh:mm:ss xx Mar 2012 ! ntp master 2 Task 2 Configure R2 to receive its clock from R1. R2 is in Dubai (+4). Configure R2 such that it automatically adjusts the clock based on the time zone R2 clock timezone DST 4 ! ntp server 192.1.10.1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 101 of 404 Task 3 Configure R3 to receive its clock from R2. R3 is located in Rome (+1). Do not use the NTP Server command to receive the clock. Do not configure any commands under the interface to accomplish this task. R3 clock timezone RST 1 ! ntp peer 192.1.23.2 Task 4 Authenticate all NTP communications using a key id of 123. The Key string should be ccie12353. R1 ntp authentication-key 123 md5 ccie12353 ntp authenticate ntp trusted-key 123 R2 ntp ntp ntp ntp R3 authentication-key 123 md5 ccie12353 authenticate trusted-key 123 server 192.1.10.1 key 123 ntp ntp ntp authentication-key 123 md5 ccie12353 authenticate trusted-key 123 server 192.1.23.2 key 123 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 102 of 404 Lab 3 – Configuring the Router for SNMP Lab Scenario: Configure a router to send SNMP traps to a configured SNMP Management Station. Limit the traps to ISAKMP and IPSec. Initial Setup: Based on the previous Lab Lab Task: Task 1 There is a SNMP Management Station located at 192.1.10.50. Configure R2 to send SNMP Traps for ISAKMP and IPSec only to this management station. It is using a community name of PublIc. R2 snmp-server host 192.1.10.50 Pub1Ic ipsec isakmp Task 2 Configure R2 to send traps to the previously configured SNMP Management station when an ISAKMP tunnel comes up or goes down. R2 snmp-server enable traps isakmp tunnel start snmp-server enable traps isakmp tunnel stop Task 3 Also configure R2 to send traps to the SNMP Management station when an IPSec tunnel comes up or goes down. R2 snmp-server enable traps ipsec tunnel start snmp-server enable traps ipsec tunnel stop Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 103 of 404 Lab 4 – Blocking Unwanted Services on the Router Lab Scenario: Disable the DHCP Server service on a Router. Initial Setup: Based on the previous Lab Lab Task: Task 1 Disable R4 from being a DHCP Server. R4 No service dhcp Task 2 R2 is sending unreachable messages if a packet is received that it cannot route. It should not send the icmp unreachable messages. Disable it on the Interface facing R3. R2 Interface F 0/1 No ip unreachables Task 3 R2 is receiving a lot of packets with the IP option fields set. You deem these packets as attack packets. Drop any packet that has the IP option field set. R2 Ip options drop Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 104 of 404 Task 4 R3 is receiving a lot of packets with the IP option fields set. You deem these packets as attack packets. Drop any packet that has the IP option field set. Allow traceroute, record-route & timestamp to work on R3. R3 Ip access-list extended SEL-OPT permit ip any any option traceroute permit ip any any option record-route permit ip any any option timestamp deny ip any any option any-options permit ip any any ! Interface F 0/0 Ip access-group SEL-OPT in Task 5 R1 is receiving a lot of packets with the source-route ip option used to control return paths. Disable this on R1. R1 No ip source-route Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 105 of 404 Lab 5 – Configuring Syslog Settings Lab Scenario: Configure the Archiving Feature on the Router to log Configuration changes to a TFTP Server. Enable Logging of changes to the running configuration file. Make sure the passwords do not get displayed when viewing the logged commands. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R1 to create Archives of your configuration files. Store them on a tftp server located at 192.1.10.100. The name of the archive should be MyConfigFiles. R1 archive path tftp://10.1.1.1/MyConfigFiles Task 2 R1 should also log changes to the running config. Make sure the password are suppressed when displaying logged commands. R1 archive log config logging enable hidekeys Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 106 of 404 CCIE Security v5 – Configuring Router & Switch Security Features Module 3 – Configuring Switch Security Features Module 3 – Configuring Security Features Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 107 of 404 Switch Lab 1 – Configuring the Port-Security Feature on the Switch SW1 R1 (.15) F 0/0 (.1) SW2 (.20) 192.1.10.0/24 VLAN 10 F 0/0 (.4) F 0/0 (.2) R4 R2 F 0/1 (.2) 192.1.23.0/24 VLAN 23 F 0/0 (.3) R3 Lab Scenario: Configuring the Port-Security feature on the Switch based on Static and Dynamic Mac-address configuration. Configure the Error Recovery feature to re-enable an error disabled port automatically. Initial Setup: Based on the previous Lab Lab Task: Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 108 of 404 Task 1 Configure SW1 such that only R1 F0/0 and R2 F0/0 can connect to Ports F 0/1 and F 0/2 respectively. If another port tries to connect to these ports they should be shudown. SW1 Interface F 0/1 Switchport port-security Switchport port-security mac xxxx.xxxx.xxxx ! Interface F 0/2 Switchport port-security Switchport port-security mac xxxx.xxxx.xxxx Task 2 Configure Port security on Ports F 0/3 – 6. You would like to learn the MAC address dynamically and copy it to the running-configuration file. SW1 Interface range F 0/3 - 6 Switchport port-security Switchport port-security mac sticky Task 3 Configure F 0/15 in VLAN 10 on SW1. Enable Port security for this ports such that 5 MAC address can be connected to it. Configure 2 MAC Address (00011010-AB12 and 0001-10101-AB13) statically. The rest of the MAC addresses can be learned dynamically. SW1 Interface F 0/15 Switchport mode access Switchport access vlan 10 Switchport port-security Switchport port-security max 5 Switchport port-security mac xxxx.xxxx.xxxx Switchport port-security mac xxxx.xxxx.xxxx Switchport port-security mac sticky Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 109 of 404 Task 4 Configure the Switch such that it tries to bring up the Port-security error disabled port automatically after 4 minutes. SW1 errdisable recovery cause psecure-violation errdisable recovery interval 240 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 110 of 404 Lab 2 – Preventing the Rogue DHCP Server Attack using the DHCP Snooping Feature Lab Scenario: Configure the DHCP Snooping feature on the switch. Initial Setup: Based on the previous Lab Lab Task: Task 1 All the SALES users will be in the SALES VLAN (100). Create this VLAN. Assign ports F 0/7 – 10 on SW2 to this VLAN. SW1 VLAN 100 SW2 Interface range F 0/7 – 10 Switchport mode access Switchport access vlan 100 Task 2 The DHCP server resides on the F 0/18 on SW2. Assign this port to the SALES VLAN. SW2 Interface F 0/18 Switchport mode access Switchport access vlan 100 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 111 of 404 Task 3 Make sure the switch only allows DHCP replies from port F 0/18 on Switch2. SW2 Ip dhcp snooping Ip dhcp snooping vlan 100 ! Interface F 0/18 Ip dhcp snooping trust Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 112 of 404 Lab 3 – Configuring Static ARP Inspection Using an ARP ACL Lab Scenario: Configuring the Switch for Static ARP Inspection to prevent ARP Spoofing attacks. Initial Setup: Based on the previous Lab Lab Task: Task 1 You have a server VLAN (200). This VLAN contains 3 Servers connected to ports F 0/11, F 0/12 and F0/13 on SW2. Create this VLAN. Assign ports F 0/11 – 13 on SW2 to this VLAN. SW1 VLAN 200 SW2 Interface range F 0/11 – 13 Switchport mode access Switchport access vlan 200 Task 2 This VLAN is under the ARP Spoofing attack. Make sure that ARP Packets are inspected. The verification should be done based on the following table: Server 1 : IP Address : 192.1.200.11 – MAC : 0001.1111.1211 Server 2 : IP Address : 192.1.200.12 – MAC : 0001.1111.1212 Server 3 : IP Address : 192.1.200.13 – MAC : 0001.1111.1213 SW2 arp access-list VLAN200 permit ip host 192.1.200.11 mac host 0001.1111.1211 permit ip host 192.1.200.12 mac host 0001.1111.1212 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 113 of 404 permit ip host 192.1.200.13 mac host 0001.1111.1213 ! ip arp inspection vlan 200 ip arp inspection filter VLAN200 vlan 200 static Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 114 of 404 Lab 4 – Configuring Dynamic ARP Inspection (DAI) Lab Scenario: Configuring the ARP Inspection feature using the MAC-IP Address database created by DHCP Snooping. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure SW2 such that it intercepts all packets received on untrusted ports in VLAN 100. It should verify valid IP-MAC mappings against the DHCP Snooping Database. This database was created by enabling DHCP Snooping for VLAN 100 in a previous lab. SW2 Ip arp inspection vlan 100 ! Interface F 0/18 Ip arp inspection trust Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 115 of 404 Lab 5 – Configuring the Source Guard Feature Lab Scenario: Configuring the Source Guard Feature to validate a device on a Switchport. Initial Setup: Based on the previous Lab Lab Task: Task 1 There is a Server connected to port F 0/7 on SW2. Turn on the IP Source Guard feature on SW2 such that only this server connects up to F 0/7. This Server has a MAC address of 0001.1010.1020 and an IP address of 192.1.50.7. SW2 ip source binding 0001.1010.1020 vlan 100 192.1.50.7 interface Fa0/7 ! Interface F 0/7 ip verify source Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 116 of 404 Lab 6 – Configuring VLAN ACL's Lab Scenario: Configuring a VLAN ACL on the Switch to control traffic by filtering based on Layer 2 & Layer 3 characteristics. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the following policy for VLAN 100 on SW1. Hosts should not be able to use the IGMP and the ICMP protocols. There is a MAC Address 0001.0012.2222 trying to attack VLAN 100. Block this MAC address from accessing any device on VLAN 100. Task 2 Use a VLAN ACL for this task. SW1 Access-list 136 permit icmp any any Access-list 136 permit igmp any any ! mac access-list extended MAC-ACL permit host 0001.0012.2222 any ! vlan access-map VLAN100 10 action drop match ip address 136 ! vlan access-map VLAN100 20 action drop match mac address MAC-ACL ! vlan access-map VLAN100 1000 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 117 of 404 action forward ! vlan filter VLAN100 vlan-list 100 on Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 118 of 404 CCIE Security v5 – Configuring Router & Switch Security Features Module 4 – Configuring IPv6 Module 4 – Configuring IPv6 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 119 of 404 Lab 1 – Configuring IPv6 with RIPng Loppback 0 FD00:1:1:1::1/64 R1 R2 F 0/0 Loppback 0 FD00:2.2.2::2/64 F 0/0 FD00:192:1:12::/64 S 0/0 FD00:192:1:23::/64 Loppback 0 FD00:4:4:4::4/64 S 0/0 Loppback 0 FD00:3:3:3::3/64 FD00:1:1:34::/64 Lo 0 F 0/0 Lo 0 F 0/0 R4 R3 Lab Scenario: Configure IPv6 Addresses on the Routers. Enable IPv6 Unicast Routing Configure RIPng as the Routing Protocol Initial Setup: None. Task 1 Enable IPv6 routing on R1,R2, R3 and R4. Assign IPv6 addresses to the F 0/0 interface of the routers as follows: R1 R1 R2 R3 R4 – – – – FD00:192:1:12::1 FD00:192:1:12::2 FD00:192:1:34::3 FD00:192:1:34::4 /64 /64 /64 /64 R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 120 of 404 ipv6 unicast-routing ! Interface F 0/0 ipv6 address FD00:192:1:12::1/64 no shut R3 Ipv6 unicast-routing ! Interface F 0/0 Ipv6 address FD00:192:1:12::2/64 No shut R4 ipv6 unicast-routing ! Interface F 0/0 ipv6 address FD00:192:1:34::3/64 no shut Ipv6 unicast-routing ! Interface F 0/0 Ipv6 address FD00:192:1:34::4/64 No shut Task 2 Configure the Loopback0 interface on all routers as follows: R1 R2 R3 R4 – – – – Loopback0 Loopback0 Loopback0 Loopback0 – – – – FD00:1:1:1::1/64 FD00:2:2:2::2/64 FD00:3:3:3::3/64 FD00:4:4:4::4/64 R1 Interface Loopback 0 Ipv6 address FD00:1:1:1::1/64 R2 Interface Loopback 0 ipv6 address FD00:2:2:2::2/64 R3 Interface Loopback 0 Ipv6 address FD00:3:3:3::3/64 R4 Interface Loopback 0 ipv6 address FD00:4:4:4::4/64 Task 3 Configure the Serial Link between R2 and R3 using the folloing IPV6 addresses: R2 – FD00:192:1:23::2/64 R3 – FD00:192:1:23::3/64 R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 121 of 404 Interface S0/0 ipv6 address FD00:192:1:23::2/64 no shut R3 Interface S0/0 ipv6 address FD00:192:1:23::3/64 no shut Task 4 Configure RIPng on all routers to route all loopbacks. Enable RIPng under the following interfaces: R1 R2 R3 R4 – – – – F F F F 0/0, 0/0, 0/0, 0/0, Loopback Loopback Loopback Loopback 0 0, S 0/0 0, S 0/0 0 R1 R2 Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable Interface Loopback 0 ipv6 rip 100 enable ! Interface S 0/0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable R4 R3 Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable ! Interface S0/0 ipv6 rip 100 enable Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 122 of 404 Lab 2 – Configuring IPv6 with EIGRP Loppback 0 FD00:1:1:1::1/64 R1 R2 F 0/0 Loppback 0 FD00:2.2.2::2/64 F 0/0 FD00:192:1:12::/64 S 0/0 FD00:192:1:23::/64 Loppback 0 FD00:4:4:4::4/64 S 0/0 Loppback 0 FD00:3:3:3::3/64 FD00:1:1:34::/64 Lo 0 F 0/0 Lo 0 F 0/0 R4 R3 Lab Scenario: Configure IPv6 Addresses on the Routers. Enable IPv6 Unicast Routing Configure EIGRP as the Routing Protocol Authenticate EIGRP Neighbor Relationships Initial Setup: Based on Previous Lab Task 1 Disable RIP NG on all routers on all interfaces. R1 R2 Interface Loopback 0 No ipv6 rip 100 enable ! Interface F 0/0 Interface Loopback 0 no ipv6 rip 100 enable ! Interface F 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 123 of 404 No ipv6 rip 100 enable No ipv6 rip 100 enable ! Interface S0/0 No ipv6 rip 100 enable R4 R3 Interface Loopback 0 no ipv6 rip 100 enable ! Interface F 0/0 No ipv6 rip 100 enable ! Interface S0/0 No ipv6 rip 100 enable Interface Loopback 0 No ipv6 rip 100 enable ! Interface F 0/0 No ipv6 rip 100 enable Task 2 Configure EIGRPv6 in AS 100 on all routers to route all loopbacks. Configure the EIGRP Router-id's as follows: R1 R2 R3 R4 – – – – 1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4 R1 R2 Interface Loopback 0 ipv6 eigrp 100 ! Interface F 0/0 ipv6 eigrp 100 ! Ipv6 router eigrp 100 Router-id 1.1.1.1 No shut Interface Loopback 0 ipv6 eigrp 100 ! Interface F 0/0 ipv6 eigrp 100 ! Interface S 0/0 Ipv6 eigrp 100 ! Ipv6 router eigrp 100 Router-id 2.2.2.2 No shut R4 R3 Interface Loopback 0 ipv6 eigrp 100 Interface F 0/0 ipv6 eigrp 100 Interface Loopback 0 ipv6 eigrp 100 ! Interface F 0/0 ipv6 eigrp 100 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 124 of 404 ! Interface S 0/0 Ipv6 eigrp 100 ! Ipv6 router eigrp 100 Router-id 3.3.3.3 No shut ! Ipv6 router eigrp 100 Router-id 4.4.4.4 No shut Task 3 Authenticate the EIGRP Neighbor relationships using MD5 authentication. Use Cisco as the Key with a key-id of 100. R1 Key Chain ABC Key 1 Key-string Cisco ! Int F 0/0 Ipv6 authentication mode eigrp 100 md5 Ipv6 authentication key-chain eigrp 100 ABC R2 Key Chain ABC Key 1 Key-string Cisco ! Int F 0/0 Ipv6 authentication Ipv6 authentication ! Int S 0/0 Ipv6 authentication Ipv6 authentication R3 mode eigrp 100 md5 key-chain eigrp 100 ABC mode eigrp 100 md5 key-chain eigrp 100 ABC Key Chain ABC Key 1 Key-string Cisco ! Int F 0/0 Ipv6 authentication mode eigrp 100 md5 Ipv6 authentication key-chain eigrp 100 ABC ! Int S 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 125 of 404 Ipv6 authentication mode eigrp 100 md5 Ipv6 authentication key-chain eigrp 100 ABC R4 Key Chain ABC Key 1 Key-string Cisco ! Int F 0/0 Ipv6 authentication mode eigrp 100 md5 Ipv6 authentication key-chain eigrp 100 ABC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 126 of 404 Lab 3 – Configuring IPv6 with OSPFv3 Loppback 0 FD00:1:1:1::1/64 R1 R2 F 0/0 Loppback 0 FD00:2.2.2::2/64 F 0/0 FD00:192:1:12::/64 S 0/0 FD00:192:1:23::/64 Loppback 0 FD00:4:4:4::4/64 S 0/0 Loppback 0 FD00:3:3:3::3/64 FD00:1:1:34::/64 Lo 0 F 0/0 Lo 0 F 0/0 R4 R3 Lab Scenario: Configure IPv6 Addresses on the Routers. Enable IPv6 Unicast Routing Configure OSPFv3 as the Routing Protocol Authenticate & Encrypt OSPFv3 Neighbor Relationships Initial Setup: Based on Previous Lab Task 1 Disable EIGRP on all routers on all interfaces. Disable the protocol on the router as well. R1 R2 Interface Loopback 0 No ipv6 eigrp100 ! Interface Loopback 0 No ipv6 eigrp100 ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 127 of 404 Interface F 0/0 No ipv6 eigrp100 ! No ipv6 router eigrp 100 R3 Interface Loopback 0 No ipv6 eigrp100 ! Interface F 0/0 No ipv6 eigrp100 ! Interface S 0/0 ! No ipv6 router eigrp 100 Interface F 0/0 No ipv6 eigrp100 ! Interface S 0/0 ! No ipv6 router eigrp 100 R4 Interface Loopback 0 No ipv6 eigrp100 ! Interface F 0/0 No ipv6 eigrp100 ! No ipv6 router eigrp 100 Task 2 Configure the routers in OSPFv3 area 0 and advertise their directly connected interfaces in this area. Configure the OSPF Router-id's as follows: R1 R2 R3 R4 – – – – 1.1.1.1 2.2.2.2 3.3.3.3 4.4.4.4 R1 R2 ipv6 router ospf 1 router-id 1.1.1.1 ! Interface Loopback0 ipv6 ospf 1 area 0 ! Interface F 0/0 ipv6 ospf 1 area 0 ipv6 router ospf 1 router-id 2.2.2.2 ! Interface Loopback0 ipv6 ospf 1 area 0 ! Interface F 0/0 ipv6 ospf 1 area 0 ! Interface S 0/0 ipv6 ospf 1 area 0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 128 of 404 R3 R4 ipv6 router ospf 1 router-id 3.3.3.3 ! Interface Loopback0 ipv6 ospf 1 area 0 ! Interface F 0/0 ipv6 ospf 1 area 0 ! Interface S 0/0 ipv6 ospf 1 area 0 ipv6 router ospf 1 router-id 4.4.4.4 ! Interface Loopback0 ipv6 ospf 1 area 0 ! Interface F 0/0 ipv6 ospf 1 area 0 Task 3 Ensure that the loopback interfaces are advertised with their correct mask. R1 R2 Interface Loopback0 ipv6 ospf network point-to-point Interface Loopback0 ipv6 ospf network point-to-point R3 R4 Interface Loopback0 ipv6 ospf network point-to-point Interface Loopback0 ipv6 ospf network point-to-point Task 4 Authenticate & encrypt the OSPF neighbor relationships between R1 and R2 using the following parameters: Encryption o IPSec o SPI : 1234 o Encryption Scheme : 3des o Key : 123456789ABC123456789ABC123456789ABC Authentication o MD5 o Key : 12345678123456781234567812345678 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 129 of 404 R1 Interface F 0/0 ipv6 ospf encryption ipsec spi 1234 esp 3des 123456789ABC123456789ABC123456789ABC123456789ABC md5 12345678123456781234567812345678 R2 Interface F 0/0 ipv6 ospf encryption ipsec spi 1234 esp 3des 123456789ABC123456789ABC123456789ABC123456789ABC md5 12345678123456781234567812345678 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 130 of 404 Lab 4 – Configuring IPv6 in IPv4 Tunnel Loppback 0 FD00:1:1:1::1/64 R1 R2 F 0/0 Loppback 0 FD00:2.2.2::2/64 F 0/0 FD00:192:1:12::/64 S 0/0 192.1.23.0/24 Loppback 0 FD00:4:4:4::4/64 S 0/0 Loppback 0 FD00:3:3:3::3/64 FD00:1:1:34::/64 Lo 0 F 0/0 Lo 0 F 0/0 R4 R3 Lab Scenario: Configure IPv6 Addresses on the Routers. Enable IPv6 Unicast Routing Configure RIPng as the Routing Protocol on the IPv6 Network Configure a IPv6IP Tunnel to connect the discontiguous IPv6 networks Initial Setup: None. Task 1 Enable IPv6 routing on R1,R2, R3 and R4. Assign IPv6 addresses to the F 0/0 interface of the routers as follows: R1 R2 R3 R4 – – – – FD00:192:1:12::1 FD00:192:1:12::2 FD00:192:1:34::3 FD00:192:1:34::4 /64 /64 /64 /64 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 131 of 404 R1 R2 ipv6 unicast-routing Interface F 0/0 ipv6 address FD00:192:1:12::1/64 no shut R3 Ipv6 unicast-routing Interface F 0/0 Ipv6 address FD00:192:1:12::2/64 No shut R4 ipv6 unicast-routing Interface F 0/0 ipv6 address FD00:192:1:34::3/64 no shut Ipv6 unicast-routing Interface F 0/0 Ipv6 address FD00:192:1:34::4/64 No shut Task 2 Configure the Loopback0 interface on all routers as follows: R1 R2 R3 R4 – – – – Loopback0 Loopback0 Loopback0 Loopback0 – – – – FD00:1:1:1::1/64 FD00:2:2:2::2/64 FD00:3:3:3::3/64 FD00:4:4:4::4/64 R1 Interface Loopback 0 Ipv6 address FD00:1:1:1::1/64 R2 Interface Loopback 0 ipv6 address FD00:2:2:2::2/64 R3 Interface Loopback 0 Ipv6 address FD00:3:3:3::3/64 R4 Interface Loopback 0 ipv6 address FD00:4:4:4::4/64 Task 3 Configure RIPng on all routers to route all loopbacks. Enable RIPng under the following interfaces: R1 – F 0/0, Loopback 0 R2 – F 0/0, Loopback 0 R3 – F 0/0, Loopback 0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 132 of 404 R4 – F 0/0, Loopback 0 R1 R2 Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable R3 R4 Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable Interface Loopback 0 ipv6 rip 100 enable ! Interface F 0/0 ipv6 rip 100 enable Task 4 Configure the Serial Link between R2 and R3 using the folloing IPv4 addresses: R2 – 192.1.23.2/24 R3 – 192.1.23.3/24 R2 Interface S0/0 ip address 192.1.23.2 255.255.255.0 clock rate 1000000 no shut R3 Interface S0/0 Ip address 192.1.23.3 255.255.255.0 no shut Task 5 Create a Tunnel between R2 and R3 Assign it an IPv6 address of FD00:192:1:23::/64. Set the Tunnel Mode to IPv6. Enable RIPng on the Tunnel Interface to connect the 2 discontiguous RIP networks. R2 R3 Interface Tunnel 23 Tunnel source S 0/0 Interface Tunnel 23 Tunnel source S 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 133 of 404 Tunnel destination 192.1.23.3 Ipv6 address FD00:192:1:23::2/64 Ipv6 enable Ipv6 rip 100 enable Tunnel mode IPV6IP No shut Tunnel destination 192.1.23.2 Ipv6 address FD00:192:1:23::3/64 Ipv6 enable Ipv6 rip 100 enable Tunnel mode IPV6IP No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 134 of 404 Lab 5 – Configuring a IPSec S-VTI Tunnel – IPv6 Lab Scenario: Configure an IPSec S-VTI Tunnel to encrypt and route traffic between 2 routers. Initial Setup: Based on the previous Lab Task 1 Configure a S-VTI tunnel interface to connect R1 to R4 using the following parameters: ISAKMP Policy: o Authentication – Pre-share o Hash – MD5 o Encryption – 3des o Group 2 o Pre-shared key : Cisco IPSec Parameters o Encryption – esp-3des o Authentication – esp-md5-hmac Tunnel Parameters: o IPv6 Address:FD00:192:1:14::/64 o Tunnel Mode : Native IPSec R1 Crypto isakmp policy 10 Authentication pre-share Hash md5 Encryption 3des Group 2 Crypto isakmp key Cisco address ipv6 FD00:192:1:34::4/64 ! Crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC ! Int tunnel 1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 135 of 404 Ipv6 address FD00:192:1:14::1/64 Tunnel source FD00:192:1:12::1 Tunnel destination FD00:192:1:34::4 Tunnel mode IPSec ipv6 Tunnel protection ipsec profile ABC R4 Crypto isakmp policy 10 Authentication pre-share Hash md5 Encryption 3des Group 2 Crypto isakmp key Cisco address ipv6 FD00:192:1:12::1/64 ! Crypto ipsec transform-set ABC esp-3des esp-md5-hmac ! crypto ipsec profile ABC set transform-set ABC ! Int tunnel 1 Ipv6 address FD00:192:1:14::4/64 Tunnel source FD00:192:1:34::4 Tunnel destination FD00:192:1:12::1 Tunnel mode IPSec ipv6 Tunnel protection ipsec profile ABC Task 2 Configure the following Loopbacks on R1 and R4: R1 – Loopback11 – FD00:11:11:11::11/64 R4 – Loopback11 – FD00:44:44:44::44/64 R1 Interface Loopback 11 ipv6 address FD00:11:11:11::11/64 R4 Interface Loopback 11 ipv6 address FD00:44:44:44::44/64 Task 3 Configure EIGRPv6 in AS 100 on R1 & R4 to route the new loopbacks (Loopback 11's on R1 & R4). Configure the EIGRP Router-id's as follows: Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 136 of 404 R1 – 1.1.1.1 R4 – 4.4.4.4 R1 R4 Interface Loopback 11 ipv6 eigrp 100 ! Interface Tunnel 1 ipv6 eigrp 100 ! Ipv6 router eigrp 100 Router-id 1.1.1.1 No shut Interface Loopback 11 ipv6 eigrp 100 ! Interface Tunnel 1 ipv6 eigrp 100 ! Ipv6 router eigrp 100 Router-id 4.4.4.4 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 137 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 1: Basic ASA Configurations on 9.X Module 1 – Basic ASA Configurations on 9.X Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 138 of 404 Lab 1 – Initializing the FW R1 F 0/0 (.1) 10.11.11.0/24 E0/1 (.10) 192.168.4.0/24 192.168.3.0/24 R3 F0/0 (.3) E0/2 (.10) E0/3 (.10) E0/0 (.10) F0/0 (.4) R4 ASA 192.1.20.0/24 F 0/0 (.2) R2 Lab Scenario: Initialize the Firewall with IP Address, Security Levels and Names of interfaces. Configure NTP to synchronize clocks. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1, R3 and R4 pointing towards the FW based on the appropriate FW Interface IP. Configure the following Loopback addresses on R1, R2, R3 & R4: o o o o R1 R1 R2 R3 R4 : : : : 10.1.1.0/24 10.2.2.0/24 10.3.3.0/24 10.4.4.0/24 R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 139 of 404 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 R3 Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut Int F 0/0 Ip address 192.168.3.3 255.255.255.0 No shut ! Int loo0 Ip add 10.3.3.3 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.168.3.10 Int F 0/0 Ip add 192.168.4.4 255.255.255.0 No shut ! Int loo 0 Ip add 10.4.4.4 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.168.4.10 R4 Lab Tasks: Task 1 Configure the ASA with the following IP configuration for the Interfaces: Interface G 0/0 G 0/1 G 0/2 G 0/3 Name Outside Inside DMZ3 DMZ4 Security Level 0 100 50 50 IP Address 192.1.20.10/24 10.11.11.10/24 192.168.3.10/24 192.168.4.10/24 At this point, the ASA should be able to ping all the surrounding routers. FW Interface G 0/0 Nameif Outside Ip address 192.1.20.10 255.255.255.0 No shut ! Interface G 0/1 Nameif Inside Ip address 10.11.11.10 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 140 of 404 ! Interface G 0/2 Nameif DMZ3 Ip address 192.168.3.10 255.255.255.0 Security-level 50 No shut ! Interface G 0/3 Nameif DMZ4 Ip address 192.168.4.10 255.255.255.0 Security-level 50 No shut Task 2 Configure the ASA to give out IP Configuration on the DMZ3 interface using the following information: IP Range : 192.168.3.51 – 192.168.3.100 DNS Server : 192.168.3.35 WINS Server : 192.168.3.36 FW dhcpd dhcpd dhcpd dhcpd dns 192.168.3.35 interface DMZ3 wins 192.168.3.36 interface DMZ3 address 192.168.3.51-192.168.3.100 DMZ3 enable DMZ3 Task 3 Configure the ASA to get the clock from R2. The ASA and R2 are located in New Delhi (GMT 5 30). R2 should be configured as the Master with a Stratum of 2. Configure it with a key id of 1 and a MD5 key of cisco. R2 Clock timezone DST 4 30 ! Do clock set 10:00:00 1 Jan 2017 *** Set the clock based on the current time using the Clock set command ! Ntp authenticate Ntp authentication-key 1 md5 cisco Ntp trusted-key 1 Ntp master 2 FW Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 141 of 404 Ntp Ntp Ntp Ntp authenticate authentication-key 1 md5 cisco trusted-key 1 server 192.1.20.2 key 1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 142 of 404 Lab 2 – Static and Default Routes Lab Scenario: Configure Default connectivity. and Static routes on the Firewall to provide Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall with Static Routes for all internal loopback networks. Internal Networks include networks off of the Inside, DMZ3 and DMZ4 interfaces. FW Route inside 10.1.1.0 255.255.255.0 10.11.11.1 Route DMZ3 10.3.3.0 255.255.255.0 192.168.3.3 Route DMZ4 10.4.4.0 255.255.255.0 192.168.4.4 Task 2 Configure a default route on the Firewall pointing towards R2. FW Route outside 0 0 192.1.20.2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 143 of 404 Lab 3 – Running RIP V2 Lab Scenario: Clear the Static Route configuration on the Routers and the Firewall. Configure RIP v2 on the Firewall. Configure MD5 authentication for RIP. Initial Setup: Based on the previous Lab Lab Task: Task 1 Clear all the static routes on the Routers and Firewall. You will be configuring Dynamic Routing protocols on them to learn routes. FW Clear configure route R1 No ip route 0.0.0.0 0.0.0.0 R2 No ip route 10.1.1.0 255.255.255.0 R3 No ip route 0.0.0.0 0.0.0.0 R4 No ip route 0.0.0.0 0.0.0.0 Task 2 Configure RIP v2 on the FW on the DMZ3 and DMZ4 interface. Disable autosummarization of routes. Also, configure RIP v2 on R3 and R4. Advertise the Loopback networks on R3 FW Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 144 of 404 Router rip No auto-summary Version 2 Network 192.168.3.0 Network 192.168.4.0 R3 Router rip No auto-summary Version 2 Network 192.168.3.0 Network 10.0.0.0 R4 Router rip No auto-summary Version 2 Network 192.168.4.0 Network 10.0.0.0 Task 3 Configure the Firewall, R3 and R4 with RIP v2 authentication using a Key 1 and password of cciesec. FW Interface G 0/2 Rip authentication mode md5 Rip authentication key cciesec key_id 1 R3 Key chain AUTH Key 1 Key-string cciesec ! Int F 0/0 Ip rip authentication mode md5 Ip rip authentication key-chain AUTH R4 Key chain AUTH Key 1 Key-string cciesec ! Int F 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 145 of 404 Ip rip authentication mode md5 Ip rip authentication key-chain AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 146 of 404 Lab 4 – Running OSPF Lab Scenario: Configure OSPF on the Firewall. Configure MD5 authentication for OSPF. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure OSPF on the outside interface of the ASA in Area 0. Hard-code the Router-id as 10.10.10.10. Also, configure OSPF on R2. Hard-code the router-id as 2.2.2.2. Have R2 advertise the Loopback network in OSPF. FW Router OSPF 1 Router-id 10.10.10.10 Network 192.1.20.0 255.255.255.0 area 0 R2 Router OSPF 1 Router-id 2.2.2.2 Network 192.1.20.0 0.0.0.255 area 0 Network 10.2.2.0 0.0.0.255 area 0 Task 2 Configure the Firewall and R2 with a key of 1 and a password of cciesec. For MD5 authentication. FW Interface G 0/0 Ospf authentication message-digest Ospf message-digeset-key 1 md5 cciesec R2 Interface F 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 147 of 404 ip Ospf authentication message-digest ip Ospf message-digeset-key 1 md5 cciesec Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 148 of 404 Lab 5 – Running EIGRP Lab Scenario: Configure EIGRP on the Firewall. Configure MD5 authentication for EIGRP. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure EIGRP on the inside interface of the Firewall in AS 100 to exchange routes with R1. Disable Auto-summarization. Advertise the R1 Loopbacks in EIGRP. FW Router EIGRP 100 No auto-summary Network 10.11.11.0 255.255.255.0 R1 Router EIGRP 100 No auto-summary Network 10.0.0.0 Network 100.0.0.0 Task 2 Configure the Firewall and R2 with EIGRP authentication using a Key 1 and password of cciesec. FW Interface G 0/1 authentication mode eigrp 100 md5 authentication key eigrp 100 cciesec key-id 1 R1 Key chain AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 149 of 404 Key 1 Key-string cciesec ! Int F 0/0 Ip authentication mode eigrp 100 md5 Ip authentication key-chain eigrp 100 AUTH Task 3 Perform Route Redistribution such that all devices have a complete picture of the entire topology. FW Router OSPF 1 Redistribute Rip subnets Redistribute EIGRP 100 subnets ! Router RIP Redistribute ospf 1 metric 1 Redistribute EIGRP 100 metric 1 ! Router EIGRP 100 Redistribute ospf 1 metric 1 1 1 1 1 Redistribute RIP metric 1 1 1 1 1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 150 of 404 Lab 6 – Configuring Management Protocols Lab Scenario: Configure the Firewall for Remote Management using Telnet and SSH. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall for Telnet Management from the Inside interface. The ASA should allow the 10.11.11.0/24 and the 10.1.1.0/24 networks to access it for management. FW telnet 10.11.11.0 255.255.255.0 inside telnet 10.1.1.0 255.255.255.0 inside Task 2 Configure the Telnet password as cciesec on the Firewall. FW Passwd cciesec Task 3 Enable SSH on the ASA. Allow R2 to connect to the ASA for Management from the outside interface using SSH Version 2. The idle timeout for SSH connections should be 2 minutes. FW Domain-name ABC.in Crypto key generate rsa ! Ssh version 2 Ssh timeout 2 Ssh 192.1.20.2 255.255.255.255 outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 151 of 404 Task 4 Create a username of ROUTER2 with a password of cciesec. Have the ASA authenticate against the Local Username database for ssh connections. FW Username ROUTER2 password cciesec ! Aaa authentication ssh console LOCAL Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 152 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 2: NAT & ACLs on 9.X Module 2 – NAT & ACLs on 9.X Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 153 of 404 Lab 1 – Configuring Basic NAT Operations R1 F 0/0 (.1) 10.11.11.0/24 ASA E0/1 (.10) 192.168.3.0/24 E0/2 (.10) F0/0 (.3) R3 E0/0 (.10) 192.1.20.0/24 F 0/0 (.2) R2 Lab Scenario: Configure Object Dynamic NAT on a Firewall Configure Object Dynamic PAT on a Firewall Configure Object Dynamic NAT with PAT Backup Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure a Default Route on R1 & R3 towards the Firewall. Configure the following Loopback addresses on R2, & R3: o R2 : 2.2.2.2/24 o R3 : 10.3.3.3/24 R1 R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 154 of 404 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Int loopback 0 Ip add 2.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut R3 Int F 0/0 Ip address 192.168.3.3 255.255.255.0 No shut ! Int loo0 Ip add 10.3.3.3 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.168.3.10 Lab Tasks: Task 1 Configure the ASA with the following IP configuration for the Interfaces: Interface G 0/0 G 0/1 G 0/2 Name Outside Inside DMZ Security Level 0 100 50 IP Address 192.1.20.10/24 10.11.11.10/24 192.168.3.10/24 At this point, the ASA should be able to ping all the surrounding routers. FW Interface G 0/0 Nameif Outside Ip address 192.1.20.10 255.255.255.0 No shut ! Interface G 0/1 Nameif Inside Ip address 10.11.11.10 255.255.255.0 No shut ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 155 of 404 Interface G 0/2 Nameif DMZ Ip address 192.168.3.10 255.255.255.0 Security-level 50 No shut Task 2 Configure a default route on the Firewall pointing towards R2. FW Route outside 0 0 192.1.20.2 Task 3 The Firewall should translate all traffic going from the DMZ towards the outside using 192.1.20.111 as the Public Address. FW object network NET-192.168.3.0 subnet 192.168.3.0 255.255.255.0 nat (DMZ,outside) dynamic 192.1.20.111 Task 4 The Firewall should translate all traffic going from 10.11.11.0/24 towards the outside using a pool of 192.1.20.151 – 192.1.20.200. FW object network POOL-10.11.11.0 range 192.1.20.151 192.1.20.200 ! object network NET-10.11.11.0 subnet 10.11.11.0 255.255.255.0 nat (inside,outside) dynamic POOL-10.11.11.0 Task 5 Create a loopback 100 on R1. Assign it an address of 10.1.1.1/24. Configure the Firewall with a static route for this network. The Firewall should translate all traffic going from this network towards outside using a pool of 192.1.20.131-192.1.20.149. Back this pool up by using a PAT address of 192.1.20.150. FW Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 156 of 404 Route inside 10.1.1.0 255.255.255.0 10.11.11.1 ! object network POOL-10.1.1.0 range 192.1.20.131 192.1.20.149 ! object network POOL-P-10.1.1.0 host 192.1.20.150 ! object-group network NAT-PAT-10.1.1.0 network-object object POOL-10.1.1.0 network-object object POOL-P-10.1.1.0 ! object network NET-10.1.1.0 subnet 10.1.1.0 255.255.255.0 nat (inside,outside) dynamic NAT-PAT-10.1.1.0 R1 Interface Loopback100 Ip address 10.1.1.1 255.255.255.0 Task 6 Create a loopback 101 on R1. Assign it an address of 10.2.2.2/24. Configure the Firewall with a static route for this network. The Firewall should translate all traffic going from this network towards outside using Outside Interface. FW Route inside 10.2.2.0 255.255.255.0 10.11.11.1 ! object network INS-NET subnet 10.2.2.0 255.255.255.0 nat (inside,outside) dynamic interface R1 Interface Loopback 101 Ip address 10.2.2.2 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 157 of 404 Task 7 Create a loopback 101 on R3. Assign it an address of 192.168.1.1/24. Configure the Firewall with a static route for this network. The Firewall should translate all traffic going from this network towards outside using a pool of 192.1.20.121-192.1.20.129. Back this pool up by using a PAT address of the outside interface. FW Route DMZ 192.168.1.0 255.255.255.0 192.168.3.3 ! object network POOL-192.168.1.0 range 192.1.20.121 192.1.20.129 ! object network NET-192.168.1.0 subnet 192.168.1.0 255.255.255.0 nat (DMZ,outside) dynamic POOL-192.168.1.0 interface Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 158 of 404 Lab 2 – Configuring Static NAT, Static Identity NAT & Static PAT Lab Scenario: Configure Object Static NAT on a Firewall Configure Object Static Identity NAT on a Firewall to override translation Configure Object Static PAT Initial Setup: Based on the previous Lab Lab Task: Task 1 Statically translate R1 such that it is seen as itself on the outside. It should not get translated. FW object network R1 host 10.11.11.1 nat (inside,outside) static 10.11.11.1 Task 2 Statically translate R3 as 192.1.20.3 on the outside. Also, translate an ACS located at 10.11.11.25 as 192.1.20.25 on the outside. FW object network R3 host 192.168.3.3 nat (DMZ,outside) static 192.1.20.3 ! object network ACS host 10.11.11.25 nat (Inside,outside) static 192.1.20.25 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 159 of 404 Task 3 Configure Static PAT on the Firewall such that if a request comes from the outside destined for an IP Address 192.1.20.7 with a port number 25, the firewall should forward the request to a SMTP server located at 192.168.3.11. If a request comes into the Firewall destined for an IP Address 192.1.20.7 with a port number 23, the Firewall should forward the request to a Device located at 192.168.3.12 for 23. FW object network S1-MAIL host 192.168.3.11 nat (dmz,out) static 192.1.20.7 service tcp 25 25 ! object network S2-TELNET host 192.168.3.12 nat (dmz,out) static 192.1.20.7 service tcp 23 23 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 160 of 404 Lab 3 – Configuring Destination NAT Lab Scenario: Configure Object Static Destination NAT Initial Setup: Based on the previous Lab Lab Task: Task 1 There is a Mainframe located on the DMZ at 192.168.3.99. Another Mainframe (200.1.1.10) from the outside needs to access it; The local Mainframe should be seen as 192.1.20.29 on the outside. The local Mainframe does not have the ability to point to a default gateway. Allow the Public Mainframe to access the local Mainframe as a local device located at 192.168.3.98. FW object network MF-LOCAL host 192.168.3.99 nat (DMZ,outside) static 192.1.20.29 ! object network MF-REMOTE host 200.1.1.10 nat (outside,DMZ) static 192.168.3.98 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 161 of 404 Lab 4 – Configuring Twice-NAT Lab Scenario: Configure Twice-NAT Policy NAT Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the ASA such that when a PC 10.1.1.1 communicates with R2 Loopback0 (2.2.2.2), it is seen as 192.1.20.21 and when it communicates with R2 F0/0 (192.1.20.2), it is seen as 192.1.20.22. FW object network HOST-10.1.1.1 host 10.1.1.1 ! object network R2 host 192.1.20.2 ! object network R2-LOOP host 2.2.2.2 ! object network HOST-10.1.1.1-R2-LOOP host 192.1.20.21 ! object network HOST-10.1.1.1-R2 host 192.1.20.22 ! nat (ins,out) source static HOST-10.1.1.1 HOST-10.1.1.1-R2-LOOP destination static R2-LOOP R2-LOOP nat (ins,out) source static HOST-10.1.1.1 HOST-10.1.1.1-R2 destination static R2 R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 162 of 404 Lab 5 – Access Control Lab Scenario: Allow traffic for the Translations that were configured in the previous lab. Configure the ICMP command to restrict pinging on the Firewall interfaces. Configure Object Groups for more efficient ACL Management. Initial Setup: Based on the previous Lab Lab Task: Task 1 Allow traffic in for R3's translated address 192.1.20.3. You should only allow traffic for Telnet, SSH and HTTP. Also allow traffic for the ACS server which was translated to 192.1.20.25 in for HTTP, TACACS+, and the RADIUS ports. FW Access-list INF permit tcp any host 192.168.3.3 eq 23 Access-list INF permit tcp any host 192.168.3.3 eq 22 Access-list INF permit tcp any host 192.168.3.3 eq 80 Access-list INF permit tcp any host 10.11.11.25 eq 80 Access-list INF permit tcp any host 10.11.11.25 eq 49 Access-list INF permit udp any host 10.11.11.25 eq 1645 Access-list INF permit udp any host 10.11.11.25 eq 1646 ! Access-group INF in interface outside Task 2 Allow traffic destined to an IP Address 192.1.20.7 (already translated) for ports SMTP and Telnet to come in. FW Access-list INF permit tcp any host 192.168.3.11 eq 25 Access-list INF permit tcp any host 192.168.3.12 eq 23 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 163 of 404 Task 3 Configure the Firewall such that only R2 Loopback 0 should be able to ping R1 F 0/0. You need to configure a static route on R2 for the 10.11.11.0/24 network to accomplish the task. FW Access-list INF permit icmp host 2.2.2.2 host 10.11.11.1 echo Access-list INF permit tcp host 192.1.20.2 host 192.168.3.3 eq 23 R2 Ip route 10.11.11.0 255.255.255.0 192.1.20.10 Task 4 Configure the Firewall such that it should be able to ping outside but nobody should be able to ping the ASA outside interface. FW Icmp permit any echo-reply outside Task 5 DMZ contains the following Application Servers and Applications: Real IP Address 192.168.3.201 192.168.3.202 192.168.3.203 192.168.3.204 192.168.3.205 192.168.3.206 192.168.3.207 Translated Address 192.1.20.201 192.1.20.202 192.1.20.203 192.1.20.204 192.1.20.205 192.1.20.206 192.1.20.207 Applications HTTP, HTTPS, FTP HTTP, HTTPS, FTP HTTP, HTTPS, FTP SMTP SMTP DNS, TFTP DNS, TFTP Task 6 Create static one-on-one translations based on the above table. FW object network S-201 host 192.168.3.201 nat (DMZ,outside) static 192.1.20.201 ! object network S-202 host 192.168.3.202 nat (DMZ,outside) static 192.1.20.202 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 164 of 404 ! object network S-203 host 192.168.3.203 nat (DMZ,outside) static ! object network S-204 host 192.168.3.204 nat (DMZ,outside) static ! object network S-205 host 192.168.3.205 nat (DMZ,outside) static ! object network S-206 host 192.168.3.206 nat (DMZ,outside) static ! object network S-207 host 192.168.3.207 nat (DMZ,outside) static 192.1.20.203 192.1.20.204 192.1.20.205 192.1.20.206 192.1.20.207 Task 7 Allow access to the Application Servers from the following networks: 101.1.1.0/24 150.1.5.0/24 175.4.1.0/24 199.1.33.0/24 215.5.7.0/24 Use the minimum number of lines possible to accomplish access to these application servers. FW Object-group network PN Network-object 101.1.1.0 255.255.255.0 Network-object 150.1.5.0 255.255.255.0 Network-object 175.4.1.0 255.255.255.0 Network-object 199.1.33.0 255.255.255.0 Network-object 215.5.7.0 255.255.255.0 ! Object-group network WEB-FTP-N Network-object host 192.168.3.201 Network-object host 192.168.3.202 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 165 of 404 Network-object host 192.168.3.203 ! Object-group network SMTP-N Network-object host 192.168.3.204 Network-object host 192.168.3.205 ! Object-group network DNS-TFTP-N Network-object host 192.168.3.206 Network-object host 192.168.3.207 ! Object-group service WEB-FTP-P tcp Port-object eq 80 Port-object eq 443 Port-object eq 21 ! Object-group service DNS-TFTP-P udp Port-object eq 69 Port-object eq 53 ! access-list INF permit tcp object-group PN object-group WEB-FTP-N object-group WEB-FTP-P access-list INF permit udp object-group PN object-group DNS-TFTP-N object-group DNS-TFTP-P access-list INF permit tcp object-group PN object-group SMTP-N eq SMTP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 166 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 3: Configuring High Availability Features Module 3 – Configuring High Availability Features Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 167 of 404 Lab 1 – Interface Redundancy R1 F 0/0 (.1) 10.11.11.0/24 E 0/1 E 0/0 ASA 192.1.20.0/24 E 0/2 F 0/0 (.2) E 0/3 192.1.30.0/24 F 0/0 (.3) R2 R3 F 0/1 (.2) F 0/1 (.3) 192.1.24.0/24 192.1.34.0/24 F 0/0.2 (.4) F 0/1 (.4) R4 Lab Scenario: Configure a Redundant Interface on the Firewall to provide Interface Level Redundancy. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1 pointing towards the FW. Configure a loopback with an IP Address of 4.2.2.2/24 on R4. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 168 of 404 Run EIGRP in AS 100 to route between R2, R3 & R4. Advertise the 192.1.20.0/24 network on R2, the 192.1.30.0/24 on R3 and the 4.2.2.0/24 network on R4 in EIGRP. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.24.2 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.20.0 Network 192.1.24.0 R4 R3 Int F 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.34.3 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.30.0 Network 192.1.34.0 Int loo 0 Ip add 4.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.24.4 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.34.4 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.24.0 Network 192.1.34.0 Network 4.0.0.0 Lab Tasks: Task 1 Configure the E 0/0 and E 0/1 as part of Redundant Interface 1 in that order. Assign it a virtual mac-address of your choice. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 169 of 404 ASA-1 Interface Redundant 1 Member-interface E 0/0 Member-interface E 0/1 Mac-address 0001.AB01.1101 ! Interface G 0/0 No shut ! Interface G 0/1 No shut Task 2 Configure ASA with the following IP configuration for the Interfaces: Interface G 0/2 G 0/3 Redundant 1 Name Outside-2 Outside-3 Inside Security Level 0 0 100 IP Address 192.1.20.10/24 192.1.30.10/24 10.11.11.10/24 ASA-1 Interface Redundant 1 Nameif inside Ip address 10.11.11.10 255.255.255.0 ! Interface G 0/2 Nameif outside-2 Ip address 192.1.20.10 255.255.255.0 No shut ! Interface G 0/3 Nameif outside-3 Ip address 192.1.30.10 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 170 of 404 Lab 2 – Route Tracking using SLA Monitor Lab Scenario: Configure Floating static routes to allow the Firewall to pick the R2 as the Primary ISP and R3 as the secondary IP. This should be configured with SLA and Object tracking to make sure that full reachability is there before it uses a particular ISP. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall such that it uses R2 as its primary Default gateway and R3 as the backup default gateway. Task 2 If the link between R2 and R4 goes down, the Firewall should use the backup default gateway to route the packets. Send SLA packet every 3 seconds. Set the timeout value to 1 second. ASA-1 SLA monitor 100 Type echo protocol ipicmpecho 4.2.2.2 interface Outside-2 Timeout 1000 Frequency 3 ! SLA monitor schedule 100 life forever start-time now ! track 10 rtr 100 reachability ! route outside-2 0.0.0.0 0.0.0.0 192.1.20.2 track 10 route outside-3 0.0.0.0 0.0.0.0 192.1.30.3 10 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 171 of 404 Lab 3 – Active / Standby Failover R1 F 0/0 (.1) 10.11.11.0/24 E 0/1 (.10) E 0/1 (.11) ASA-1 ASA-2 E 0/0 (.10) E 0/0 (.11) 192.1.20.0/24 F 0/0 (.2) R2 Lab Scenario: Configure Stateless Active/Standby Failover. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1 pointing towards the FW. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 172 of 404 Lab Tasks: Task 1 FW-1 and FW-2 will be configured in a Active/Standby Failover Setup. FW-1 will be the Primary Firewall and FW-2 will be the Secondary Firewall. Use the following parameters for the Failover configurations: Failover Failover Failover Failover Failover LAN Interface : E 0/2 Interface Name : FC IP Addresses Active : 10.10.10.1/24 IP Addresses Standby : 10.10.10.2/24 Key : cisco123 FW-1 Interface G 0/2 No shutdown ! Failover lan enable (In case of PIX Firewall) Failover lan interface FC E0/2 Failover interface IP FC 10.10.10.1 255.255.255.0 standby 10.10.10.2 Failover key cisco123 Failover lan unit primary Failover FW-2 Interface G 0/2 No shutdown ! Failover lan enable (In case of PIX Firewall) Failover lan interface FC E0/2 Failover interface IP FC 10.10.10.1 255.255.255.0 standby 10.10.10.2 Failover key cisco123 Failover lan unit secondary Failover Task 2 Configure FW-1 with the following Primary and Standby IP Addresses: Interface G 0/0 G 0/1 Name Outside Inside Security Level 0 100 System IP 192.1.20.10/24 10.11.11.10/24 Standby IP 192.1.20.11/24 10.11.20.11/24 FW-1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 173 of 404 Interface G 0/0 Ip address 192.1.20.10 255.255.255.0 standby 192.1.20.11 Nameif Outside No shut ! Interface G 0/1 Ip address 10.11.11.10 255.255.255.0 standby 10.11.11.11 Nameif inside No shut Task 3 Configure RIP v2 as the routing protocol on both the Routes and the Firewall. Configure an Loopback interface 10.1.1.1/24 on R1 and 10.2.2.2/24 on R2. Advertise them under RIP. R1 Interface Loopback 0 Ip address 10.1.1.1 255.255.255.0 ! Router rip No auto-summary Version 2 Network 10.0.0.0 R2 Interface Loopback 0 Ip address 10.2.2.2 255.255.255.0 ! Router rip No auto-summary Version 2 Network 10.0.0.0 Network 192.1.20.0 FW-1 Router Rip Version 2 No auto-summary Network 10.0.0.0 Network 192.1.20.0 Task 4 Allow the inside networks to go out using a Outside pool of 192.1.20.51 – 192.1.20.100. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 174 of 404 FW-1 Global (outside) 1 192.1.20.51-192.1.20.100 Nat (inside) 1 0 0 Note: If you do Show Run on FW-2, all the configuration should have replicated over to it. Also, do Show Failover to verify the Failover status. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 175 of 404 Lab 4 – Stateful Failover Lab Scenario: Configure Statefull Failover between FW-1 & FW-2. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure G 0/3 as the Failover link to replicated the State and connection information from the Active Firewall to the Standby firewall. Configure E 0/3 with an IP Address of 10.20.20.1/24 as the Active Address and 10.20.20.2/24 as the Standby address. Assign it a name of SFF. FW-1 Interface G 0/3 No shut ! Failover link G 0/3 SFF Failover interface IP SFF 10.20.20.1 255.255.255.0 standby 10.20.20.2 ***Note : This only needs to be done on the Active device as the configuration will be replicated to the standby box Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 176 of 404 Lab 5 – Security Contexts on the ASA using Shared Interface R1 F 0/0 (.1) 192.1.100.0/24 VLAN 100 E 0/0 (.21) (Shared) E 0/0 (.11) (Shared) R4 10.40.40.0/24 ASA1-C1 F 0/0 (.4) ASA1-C2 E 0/1.4 (.11) E 0/1.2 (.11) 10.20.20.0/24 E 0/1.3 (.21) 10.30.30.0/24 F 0/0 (.2) R2 F 0/0 (.3) R3 Lab Scenario: Configure a FW in Multi-context mode. Configure Shared Interfaces with manual mac-address assignment. Configure Resource-based class-map to limit the resources to a particular context. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure a Loopback 4.2.2.2/24 on R1 to simulate the internet. Configure Default Routes on R2, R3 & R4 pointing towards the appropriate Firewall address. Configure the Switch interface connected to the Router Interfaces in the appropriate VLANs. Use VLANs of your choice. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 177 of 404 R1 R2 Int loopback 0 Ip address 4.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 192.1.100.1 255.255.255.0 No shut R3 Int F 0/0 Ip address 10.20.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.20.20.11 Int F 0/0 Ip address 10.30.30.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.30.30.11 SW Int F 0/0 Ip address 10.40.40.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.40.40.11 R4 Interface F 0/1 Description Connected to R1 Switchport mode access Switchport access vlan 100 ! Interface F 0/2 Description Connected to R2 Switchport mode access Switchport access vlan 20 ! Interface F 0/3 Description Connected to R3 Switchport mode access Switchport access vlan 30 ! Interface F 0/4 Description Connected to R4 Switchport mode access Switchport access vlan 40 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 178 of 404 Lab Tasks: Task 1 Configure both FW's for Multiple Contexts. The Second one will be used later for Active/Active Failover FW-1 FW-2 Mode multiple Mode multiple Task 2 Bring up the interfaces E0/0 and E 0/1. Split E 0/1 into 3 sub-interfaces based on the Network diagram on FW-1. Configure the Switch to assign the Firewall ports to the appropriate VLANs or Trunk Ports. FW-1 Interface E 0/0 No shut ! Interface E 0/1 No shut ! interface E 0/1.2 Vlan 20 interface E 0/1.3 Vlan 30 interface E 0/1.4 Vlan 40 Switch Interface F 0/10 Description Connected to FW-1 E0/0 Switchport mode access Switchport access vlan 100 ! Interface F 0/11 Description Connected to FW-1 E0/1 Switchport trunk encapsulation dot1q Switchport mode trunk Task 3 Configure two contexts on FW-1. Name them as VFW1 and VFW2. Configure them with configuration files VFW1.cfg and VFW2.cfg respectively on Flash. Allocate the appropriate interface to the appropriate contexts based on the Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 179 of 404 Network Diagram. (Note: Delete any existing .cfg files in flash before creating the context) FW-1 Context VFW1 Allocate-interface E0/0 Allocate-interface E0/1.2 Allocate-interface E0/1.4 Config-url flash:VFW1.cfg ! Context VFW2 Allocate-interface E0/0 Allocate-interface E0/1.3 Config-url flash:VFW2.cfg Task 4 Configure Virtual-Mac addresses of your choice on the shared interface to allow the FW to classify the traffic using the MAC- Address. Configure Interfaces in Context VFW1 as follows: Interface E 0/0 E 0/1.2 E 0/1.4 Name Outside (Shared) Inside DMZ Security Level 0 100 50 IP Address 192.1.100.11/24 10.20.20.11/24 10.40.40.11/24 FW-1 Changeto context VFW1 Interface E 0/0 Nameif outside Ip address 192.1.100.11 255.255.255.0 Mac-address 0001.1111.1111 ! Interface E 0/1.2 Nameif Inside Ip address 10.20.20.11 255.255.255.0 ! Interface E 0/1.4 Nameif DMZ Security-level 50 Ip address 10.40.40.11 255.255.255.0 Task 5 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 180 of 404 Configure Virtual-Mac addresses of your choice on the shared interface to allow the FW to classify the traffic using the MAC- Address. Configure Interfaces in Context VFW2 as follows: Interface E 0/0 E 0/1.3 Name Outside (Shared) Inside Security Level 0 100 IP Address 192.1.100.21/24 10.30.30.21/24 FW-1 Changeto context VFW2 Interface E 0/0 Nameif outside Ip address 192.1.100.21 255.255.255.0 Mac-address 0001.222.2221 ! Interface E 0/1.3 Nameif Inside Ip address 10.30.30.21 255.255.255.0 Task 6 Enable NAT-control on VFW1. Configure VFW1 to allow the inside network access to the outside networks using Dynamic Translation. Use a pool of 192.1.100.51 – 192.1.100.69. Backup the NAT pool with a PAT Pool using an IP Address of 192.1.100.70. R2 should be seen as 192.1.100.2 on the outside network. FW-1 Changeto context VFW1 Nat-control ! global (outside) 1 192.1.100.51-192.1.100.69 global (outside) 1 192.1.100.70 ! nat (inside) 1 10.20.20.0 255.255.255.0 static (inside,outside) 192.1.100.2 10.20.20.2 Task 7 Configure VFW2 to allow the inside network access to the outside networks using Dynamic Translation. Use a pool of 192.1.100.71 – 192.1.100.89. Backup the NAT pool with a PAT Pool using an IP Address of 192.1.100.90. Create a Static Translation for R3 as 192.1.100.3 as the Translated address on the Outside interface. FW-1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 181 of 404 Changeto context VFW2 global (outside) 1 192.1.100.71-192.1.100.89 global (outside) 1 192.1.100.90 ! nat (inside) 1 10.22.22.0 255.255.255.0 ! static (inside,outside) 192.1.100.3 10.30.30.3 Task 8 Allow R2 to Telnet to R3 and vice versa. FW-1 Changeto context VFW1 Access-list INF permit tcp host 192.1.100.3 host 192.1.100.2 eq 23 ! Access-group INF in interface outside Changeto context VFW2 Access-list INF permit tcp host 192.1.100.2 host 192.1.100.3 eq 23 ! Access-group INF in interface outside Task 9 Configure resource allocation for VFW-2 based on the following: Maximum Connections : 100 Maximum Telnet & ASDM Connections each : 3 Maximum Xlate entries : 100 FW-1 Changeto system class CM-VFW2 limit-resource Conns 100 limit-resource Telnet 3 limit-resource ASDM 3 limit-resource Xlates 100 ! context VFW2 member CM-VFW2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 182 of 404 Lab 6 – Active/Active Failover R1 (.1) 192.1.100.0/24 VLAN 100 10.44.44.0/24 VLAN 40 (.22) (.11) ASA-1 C1 C2 (.12) (.21) C1 ASA-2 C2 R4 (.11) (.4) (.12) (.11) (.12) (.22) (.21) 10.22.22.0/24 VLAN 20 (.2) R2 10.22.22.0/24 VLAN 30 F 0/1.2 (.11) (.3) R3 Lab Scenario: Configure Active/Active Failover with VFW1 Active on FW-1 & VFW2 active on FW-2. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure FW-2 to back up FW-1 from the previous lab. Configure E 0/2 as the Failover Link. This interface will be used to transmit Failover control messages. Assign it a name of FC. Also assign it an active IP address of 10.100.100.1/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 183 of 404 with a standby address of 10.100.100.2. Authenticate the Failover Control messages using a Key of cciesec. FW-1 Changeto system Interface E 0/2 No shutdown !

Failover lan interface FC E0/2 Failover interface IP FC 10.100.100.1 255.255.255.0 standby 10.100.100.2 Failover key cciesec Failover lan unit primary ASA-2 Interface E 0/2 No shutdown ! Failover lan interface FC E0/2 Failover interface IP FC 10.100.100.1 255.255.255.0 standby 10.100.100.2 Failover key cciesec Failover lan unit secondary *** Note: We did not enable Failover yet. We will wait until the entire Active/Active configuration is done before enabling it. Task 2 Configure Failover in such a way that VFW1 will try to become Active on FW-1 if it is up and VFW2 will try to become Active on FW-2 if it is up. FW-1 failover group 1 preempt failover group 2 secondary preempt ! Context ASA-C1 Join-failover-group 1 ! Context ASA-C2 Join-failover-group 2 ***Note: This configuration only needs to be done on the Active/Primary box. It will be replicated when Failover is established. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 184 of 404 Task 3 Configure E 0/2 also to transmit State and connection information to the Standby box. FW-1 Failover link FC E0/2 ! Failover FW-2 Failover ***Note: The Stateful Failover configuration is only done on the Active/Primary box. Once, we have setup all the failover configuration commands on the appropriate boxes, we enable failover on both the boxes. Type Show Failover to make sure that VFW1 (Group 1) is active on FW-1 and VFW-2 (Group 2) is active on FW-2. Task 4 Configure the Switch to assign the appropriate ports to the appropriate VLANS for FW-2 and the Failover Interface for FW-1. Switch Interface F 0/12 Description Connected to FW-1 E0/2 Switchport mode access Switchport access vlan 110 ! Interface F 0/15 Description Connected to FW-2 E0/0 Switchport mode access Switchport access vlan 100 ! Interface F 0/16 Description Connected to FW-2 E0/1 Switchport trunk encapsulation dot1q Switchport mode trunk ! Interface F 0/17 Description Connected to FW-2 E0/2 Switchport mode access Switchport access vlan 110 Task 5 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 185 of 404 Re-Configure VFW-1 on FW-1 with the following Primary and Standby IP Addresses for VFW1: Interface E 0/0 E 0/1.2 E 0/1.4 Name Outside Inside DMZ Security Level 0 100 50 System IP 192.1.100.11/24 10.20.20.11/24 10.40.40.11/24 Standby IP 192.1.100.12/24 10.20.20.12/24 10.40.40.12/24 FW-1 Changeto context VFW1 Interface E 0/0 IP Address 192.1.100.11 255.255.255.0 standby 192.1.100.12 ! Interface E 0/1.2 IP Address 10.20.20.11 255.255.255.0 standby 10.20.20.12 ! Interface E 0/1.4 IP Address 10.40.40.11 255.255.255.0 standby 10.40.40.12 Task 6 Re-Configure VFW-2 on FW-2 with the following Primary and Standby IP Addresses for VFW2: Interface E 0/0 E 0/1.3 Name Outside Inside Security Level 0 100 System IP 192.1.100.21/24 10.30.30.21/24 Standby IP 192.1.100.22/24 10.30.30.22/24 FW-2 Changeto context VFW2 Interface E 0/0 IP Address 192.1.100.21 255.255.255.0 standby 192.1.100.22 ! Interface E 0/1.3 IP Address 10.30.30.21 255.255.255.0 standby 10.30.30.22 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 186 of 404 Lab 7 – Port Channels R1 F 0/0 (.1) 10.11.11.0/24 VLAN 10 G 0/1 G 0/0 ASA 192.1.20.0/24 VLAN 20 E 0/2 F 0/0 (.2) R2 Lab Scenario: Configure a Port Channel on a Firewall. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1 pointing towards the FW. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Lab Tasks: Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 187 of 404 Task 1 Configure the E 0/0 and E 0/1 as part of Port Channel 1. ASA-1 Interface G 0/0 Channel-group 1 mode active No shut ! Interface G 0/1 Channel-group 1 mode active No shut Task 2 Configure ASA with the following IP configuration for the Interfaces: Interface G 0/2 Port-Channel 1 Name Outside Inside Security Level 0 100 IP Address 192.1.20.10/24 10.11.11.10/24 ASA-1 Interface Port-Channel 1 Nameif Inside Ip address 10.11.11.10 255.255.255.0 ! Interface G 0/2 Nameif Outside Ip address 192.1.20.10 255.255.255.0 No shut Task 3 Configure the devices in the appropriate VLAN's on the Switch(s). SW Interface range F 0/1 , F 0/10 – 11 Switchport mode access Switchport access vlan 11 *** Put the E 0/0 & E 0/1 ports of the Firewall and R1 F0/0 in the same VLAN. You might have these ports on different switches based on your physically topology. ! Interface range F 0/2 , F 0/12 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 188 of 404 Switchport mode access Switchport access vlan 20 *** Put the Outside Port of the Firewall and R2 F0/0 in the same VLAN. You might have these ports on different switches based on your physically topology. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 189 of 404 Lab 8 – Clustering – Individual Interface Mode R2 F 0/0 (.1) 192.1.20.0/24 – VLAN 20 G 0/3 (.12) G 0/3 (.13) ASA-1 ASA-2 G 0/1 (.12) G 0/1 (.13) 10.11.11.0/24 – VLAN 10 F 0/0 (.2) R2 Lab Scenario: Configure a Firewall Cluster using Physical Interfaces. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Interface Loopback0 Ip address 1.1.1.1 255.0.0.0 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 190 of 404 Lab Tasks: Task 1 FW-1 and FW-2 will be configured in a Cluster. FW-1 will be the Master Firewall and FW-2 will be the Slave Firewall. Use the following parameters for the Failover configurations: Cluster Interface Mode: Individual Cluster Group Name: CCIEv5 Failover LAN Interface : G 0/0 Failover IP Addresses Master : 10.10.10.1/24 Failover IP Addresses Slave : 10.10.10.2/24 Failover Key : cisco123 FW-1 Cluster Interface-mode Individual force ! Interface G 0/0 No shutdown ! Cluster group CCIEv5 local-unit PRI cluster-interface GigabitEthernet0/0 ip 10.10.10.1 255.255.255.0 priority 1 key cisco123 enable noconfirm FW-2 Cluster Interface-mode Individual force ! Interface G 0/0 No shutdown ! Cluster group CCIEv5 local-unit SEC cluster-interface GigabitEthernet0/0 ip 10.10.10.2 255.255.255.0 priority 10 key cisco123 enable noconfirm Note: Type show cluster info to see the Status of the devices in the cluster. Task 2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 191 of 404 Configure Switch ports connecting towards the Gig 0/3 Interfaces of the 2 ASA's and R2 in VLAN 20. Configure Switch ports connecting towards the Gig 0/1 Interfaces of the 2 ASA's and R1 in VLAN 10. SW1 Interface range Gig 1/0/1, Gig 1/0/11, Gig 1/0/13 Switchport mode access Switchport access vlan 10 ! Interface Gig 1/0/2 Switchport mode access Switchport access vlan 20 SW2 Interface range Fast 5/0/12, Fast 5/0/14 Switchport mode access Switchport access vlan 20 Task 3 Configure FW-1 Interfaces based on the following table: Interface Gig 0/3 Name Outside Security Level 0 Gig 0/1 Inside 100 Master IP/Pool 192.1.20.11/24 Pool: 192.1.20.12-14 10.11.11.11/24 Pool: 10.11.11.12-14 FW-1 Ip local pool OUTSIDE 192.1.20.12-192.1.20.14 Ip local pool INSIDE 10.11.11.12-10.11.11.14 ! Interface Gig 0/3 Nameif Outside Ip address 192.1.20.11 255.255.255.0 cluster-pool OUTSIDE No shut ! Interface Gig 0/1 Nameif Inside Ip address 10.11.11.11 255.255.255.0 cluster-pool INSIDE No shut Task 4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 192 of 404 Configure EIGRP as the routing protocol is AS 100 on both the Routers and the Firewall. Configure a Loopback interface 1.1.1.1/24 on R1 and 2.2.2.2/24 on R2. Advertise them under RIP. R1 Interface Loopback 0 Ip address 1.1.1.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 10.11.11.0 0.0.0.255 Network 1.0.0.0 R2 Interface Loopback 0 Ip address 10.2.2.2 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 2.2.2.0 0.0.0.255 Network 192.1.20.0 FW-1 Router EIGRP 100 No auto-summary Network 10.11.11.0 255.255.255.0 Network 192.1.20.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 193 of 404 Lab 9 – Clustering – Spanned Interface Mode R2 F 0/0 (.1) 192.1.20.0/24 – VLAN 20 PO 20 [.11] G 0/3 G 0/3 ASA-1 ASA-2 G 0/1 (.12) G 0/1 (.13) PO 10 [.11] 10.11.11.0/24 – VLAN 10 F 0/0 (.2) R2 Lab Scenario: Configure a Firewall Cluster using Spanned Port-channel Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1 pointing towards the FW. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 194 of 404 ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Lab Tasks: Task 1 FW-1 and FW-2 will be configured in a Cluster. FW-1 will be the Master Firewall and FW-2 will be the Slave Firewall. Use the following parameters for the Failover configurations: Cluster Interface Mode: Spanned Cluster Group Name: CCIEv5 Failover LAN Interface : G 0/0 Failover IP Addresses Master : 10.10.10.1/24 Failover IP Addresses Slave : 10.10.10.2/24 Failover Key : cisco123 FW-1 Cluster Interface-mode spanned force ! Interface G 0/0 No shutdown ! Cluster group CCIEv5 local-unit PRI cluster-interface GigabitEthernet0/0 ip 10.10.10.1 255.255.255.0 priority 1 key cisco123 enable noconfirm FW-2 Cluster Interface-mode spanned force ! Interface G 0/0 No shutdown ! Cluster group CCIEv5 local-unit SEC cluster-interface GigabitEthernet0/0 ip 10.10.10.2 255.255.255.0 priority 10 key cisco123 enable noconfirm Note: Type show cluster info to see the Status of the devices in the Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 195 of 404 cluster. Task 2 Configure FW-1 Ports and the correcponding switch ports in an Port-channel based on the following table: Interface G 0/1 G 0/3 Port-channel 10 20 Protocol LACP LACP VLAN 10 20 FW-1 Interface G 0/1 Channel-group 10 mode active No shut ! Interface G 0/3 Channel-group 20 mode active No shut SW1 Interface range Gig 1/0/11, Gig 1/0/13 Channel-group 10 mode active No shut ! Interface Port-channel 10 switchport mode access switchport access vlan 10 ! Interface Gig 1/0/1 Switchport mode access Switchport acces vlan 10 ! Interface Gig 1/0/2 Switchport mode access Switchport acces vlan 20 SW2 Interface range Gig 1/0/12, Gig 1/0/14 Channel-group 20 mode active No shut ! Interface Port-channel 20 switchport mode access switchport access vlan 20 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 196 of 404 Task 3 Configure FW-1 Port-channel Interfaces based on the following table Interface Port-channel 20 Port-channel 10 Name Outside Inside Security Level 0 100 System IP 192.1.20.11/24 10.11.11.11/24 FW-1 Interface Port-channel 20 Port-channel span-cluster Ip address 192.1.20.11 255.255.255.0 Nameif Outside Mac-address aaaa.bbbb.cc20 No shut ! Interface Port-channel 10 Port-channel span-cluster Ip address 10.11.11.11 255.255.255.0 Nameif Inside Mac-address aaaa.bbbb.cc10 No shut Task 4 Configure EIGRP as the routing protocol is AS 100 on both the Routers and the Firewall. Configure a Loopback interface 1.1.1.1/24 on R1 and 2.2.2.2/24 on R2. Advertise them under RIP. R1 Interface Loopback 0 Ip address 1.1.1.1 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 10.11.11.0 0.0.0.255 Network 1.1.1.0 0.0.0.255 R2 Interface Loopback 0 Ip address 10.2.2.2 255.255.255.0 ! Router EIGRP 100 No auto-summary Network 2.2.2.0 0.0.0.255 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 197 of 404 Network 192.1.20.0 FW-1 Router EIGRP 100 No auto-summary Network 10.11.11.0 255.255.255.0 Network 192.1.20.0 Task 5 Allow the inside networks to go out using a Outside pool of 192.1.20.51 – 192.1.20.100. FW-1 Object network POOL-A Range 192.1.20.51 192.1.20.100 ! Object network INS-NET Subnet 10.11.11.0 255.255.255.0 Nat (inside,outside) dynamic POOL-A Note: If you do Show Run on FW-2, all the configuration should have replicated over to it. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 198 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 4: Deep Packet Inspection Module 4 – Deep Packet Inspection Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 199 of 404 Lab 1 – Configuring System L7 Deep Packet Inspection R1 F 0/0 (.1) 10.11.11.0/24 G 0/1 (.10) Inside ASA G 0/0 (.10) Outside 192.1.20.0/24 F 0/0 (.2) R2 Lab Scenario: Configure System Based Layer 7 Inspection for FTP & EMSTP on NonStandard Ports. Configure ICMP Inspection. Initial Setup: Configure the IP Addresses based on the Diagram. Configure the following Static Routes on the appropriate routers: o Default Routes on R1 pointing towards FW. o Default Route on the FW towards R2. Configure the following Loopback addresses on R1 & R2: o R1 : 200.1.1.0/24 o R2 : 200.2.2.0/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 200 of 404 R1 R2 Int loopback 0 Ip add 200.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 FW Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut Int G 0/0 Nameif Outside Ip add 192.1.20.10 255.255.255.0 No shut ! Int G 0/1 Nameif Inside Ip add 10.11.11.10 255.255.255.0 No shut ! Route outside 0 0 192.1.20.2 Lab Tasks: Task 1 Configure Dynamic NAT on the Firewall to allow in the inside users to go out using a pool of 192.1.20.51-192.1.20.100. FW Object network POOL-A Range 192.1.20.51-192.1.20.100 ! Object network INS-NET Subnet 10.11.11.0 255.255.255.0 Nat (inside,outside) dynamic pool POOL-A Task 2 Configure FTP to be inspected on port 2100 in addition to port 21. Do not use any access-list for this task. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 201 of 404 FW Class CM4-FTP2100 Match port tcp eq 2100 ! policy-map global_policy class CM4-FTP2100 inspect ftp Task 3 Configure SMTP to be inspected on port 2500 in addition to port 25. Do not use any access-list for this task. FW Class CM4-SMTP2500 Match port tcp eq 2500 ! policy-map global_policy class CM4-SMTP2500 inspect esmtp Task 4 Enable Application inspection in the Default inspection policy for the ICMP so that inside users can ping outside the firewall. ASA policy-map global_policy class inspection_default inspect icmp Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 202 of 404 Lab 2 – Configuring User Defined L7 Deep Packet Inspection Lab Scenario: Configure User-defined L7 Deep Packet inspection for FTP. Configure User-defined L7 Deep Packet inspection for HTTP. Configure User-defined L7 Deep Packet inspection for ESMTP. Configure User-defined L7 Deep Packet inspection for IPSEC. Initial Setup: Based on the previous Lab Lab Task: Task 1 There is a FTP Server located at 10.11.11.221. Translate this server as 192.1.20.221 on the outside. Allow FTP traffic to this Server from the outside. FW Object network FTP Host 10.11.11.221 Nat (inside,outside) static 192.1.20.221 ! access-list INF permit tcp any host 10.11.11.221 eq 21 ! Access-group INF in interface outside Task 2 FTP traffic connections to this server should be reset if they are trying to execute the following commands: Put Rmd Rnfr dele FW Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 203 of 404 Policy-map type inspect FTP PM7-FTPCMD Match-request command put rmd rnfr dele Reset ! access-list FTP-S permit tcp any host 10.11.11.221 eq 21 ! class-map CM4-MYFTP match access-list FTP-S ! policy-map global_policy class CM4-MYFTP inspect FTP strict PM7-FTPCMD Task 3 There is a HTTP Server located at 10.11.11.222. Translate this server as 192.1.20.222 on the outside. Allow Web traffic to this Server from the outside. FW Object network WWW Host 10.11.11.222 Nat (inside,outside) static 192.1.20.222 ! access-list INF permit tcp any host 10.11.11.222 eq 80 Task 4 Deny any web traffic that has any of the following characteristics coming into the server: • The word CMD anywhere in the URL. • The word BOMB anywhere in the URL. • If the packet has request header length greater than 250 bytes. FW Regex RE-CMD "CMD" Regex RE-BOMB "BOMB" ! Class-map type inspect http match-any CM7-RE-WEB Match request URI regex RE-CMD Match request URI regex RE-BOMB Match request header length gt 250 ! policy-map type inspect http PM7-RE-WEB class CM7-RE-WEB Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 204 of 404 reset ! access-list HTTP-S permit tcp any host 192.1.20.222 eq 80 ! class CM4-RE-WEB match access-list HTTP-S ! policy-map global_policy class CM4-RE-WEB inspect http PM7-RE-WEB Task 5 Configure your firewall to drop all e-mails that are greater the 1 MB in size. Do not create a new class for this. FW policy-map type inspect esmtp PM7-MAIL match body length gt 1000000 reset ! policy-map global_policy class inspection_default no inspect esmtp inspect esmtp PM7-MAIL Task 6 Configure your firewall to limit the number of ESP connections from the same client to 25. Do not create a new class for it. FW policy-map type inspect ipsec-pass-thru PM7-ESP parameters esp per-client-max 25 ! policy-map global_policy class inspection_default inspect ipsec-pass-thru PM7-ESP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 205 of 404 Lab 3 – Configuring TCP Normalization Lab Scenario: Allow BGP neighbor relationship with MD5 authentication to form between 2 Routers thru the Firewall. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a BGP Neighbor relationship between R1 and R2. They should be in AS 100. They should advertise their local loopback interfaces to each other. Configure a static route on R2 for the 10.11.11.0 network to provide connectivity. Also create a static route for the 192.1.20.0 network. Although, R1 has a default route, BGP needs a static route to build a neighbor relationship. R1 Router BGP 100 Network 200.1.1.0 Neighbor 192.1.20.2 remote-as 100 ! Ip route 192.1.20.0 255.255.255.0 10.11.11.10 R2 Router BGP 100 Network 200.2.2.0 Neighbor 10.11.11.1 remote-as 100 ! Ip route 10.11.11.0 255.255.255.0 192.1.20.10 *** Notice that you did not need to open up any ports on the firewall to accomplish this. This is due to the fact that BGP is tcp-based and the internal neighbor will send a BGP neighbor request to R2. Because of the Implicit TCP inspection, the return packet will be allowed and the neighbor relationship will be formed. Task 2 Authenticate the BGP neighbor relationship using a password of cisco. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 206 of 404 R1 Router BGP 100 Neighbor 192.1.20.2 password cisco R2 Router BGP 100 Neighbor 10.11.11.1 password cisco *** Notice that after specifying the MD5 authentication, the neighbor relationship goes down. To understand this, you need to understand what authentication does. Authentication creates a hash (Like a checksum) of the packet and puts it in a unused TCP header field (Option 19). The hash is used to make sure that the packet was not tampered (changed) during transit. There are 2 reasons for the break. Number 1: The firewall randomizes (Changes) the TCP sequence number. This breaks the hash. Number 2: The Option field is cleared by the TCP Normalization process. To fix it, we modify the default behavior of the TCP Normalization field. Task 3 Modify the default TCP Randomization parameters to allow the BGP Authentication to take place. FW TCP-map BGPMAP TCP-options range 19 19 allow ! class-map BGP match port tcp eq 179 ! policy-map global_policy class BGP set connection random-sequence-number disable set connection advanced-options BGPMAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 207 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 5: Transparent Firewalls on 9.X Module 5 – Transparent Firewalls on 9.X Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 208 of 404 Lab 1 – Configuring a Transparent Firewall on ASA 9.x R1 F 0/0 (.1) 10.11.11.0/24 VLAN 11 G 0/1 Inside ASA G 0/0 Outside 10.11.11.0/24 VLAN 22 F 0/0 (.2) R2 F 0/1 (.2) 192.1.23.0/24 VLAN 23 F 0/0 (.3) R3 Lab Scenario: Initialize the Firewall as Layer 2 Firewall Transparent Firewall. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure Default Routes on R1 pointing towards R2. Configure a Default Gateway on R2 towards R3. Configure the following Loopback addresses on R1, R2 & R3: o R1 : 10.1.1.0/24 o R2 : 10.2.2.0/24 o R3 : 3.3.3.3/8 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 209 of 404 R1 R2 Int loopback 0 Ip add 10.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.2 Int loopback 0 Ip add 10.2.2.2 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.1.23.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.3 R3 Int loopback 0 Ip add 3.3.3.3 255.255.255.0 ! Int F 0/0 Ip add 192.1.23.3 255.255.255.0 No shut Lab Tasks: Task 1 Configure the Firewall as a Transparent Firewall. FW Firewall Transparent Task 2 Configure G 0/0 as the outside interface with a security level of 0. Bring the Interface up. Configure G 0/1 as the inside interface with a security level of 100. Configure them to be part of the same bridge group. Bring the Interfaces up. FW Interface G 0/0 Nameif outside Bridge-group 1 No shutdown Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 210 of 404 ! Interface G 0/1 Nameif inside Bridge-group 1 No shutdown Task 3 Configure the devices in the appropriate VLAN's on the Switch(s). SW Interface range F 0/1 , F 0/11 Switchport mode access Switchport access vlan 11 *** Put the Inside Port of the Firewall and R1 F0/0 in the same VLAN. You might have these ports on different switches based on your physically topology. ! Interface range F 0/2 , F 0/10 Switchport mode access Switchport access vlan 22 *** Put the Outside Port of the Firewall and R2 F0/0 in the same VLAN. You might have these ports on different switches based on your physically topology. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 211 of 404 Lab 2 – Configuring Management on a Transparent FW Lab Scenario: Configure the Firewall for Remote Management using Telnet. Initial Setup: Based on the previous Lab Lab Task: Task 1 Assign the Firewall an IP address of 10.11.11.10/24 to the bridge-group created in the previous lab. Configure the Firewall with a default gateway of 10.11.11.2. FW Interface BVI 1 IP address 10.11.11.10 255.255.255.0 ! Route outside 0 0 10.11.11.2 Task 2 Allow Management of the Firewall only from VLAN 11 devices. Telnet and SSH access to the ASA should be allowed from the inside interface only. FW Domain-name ABC.in ! crypto key generate rsa ! telnet 10.11.11.0 255.255.255.0 inside ssh 10.11.11.0 255.255.255.0 inside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 212 of 404 Lab 3 – ACL's in Transparent Mode Lab Scenario: Configure L2 & L3 ACL's on the transparent firewall to control flow of traffic thru it. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall to allow R2 and R1 to communicate to each other to exchange Routing information. Configure R1 and R2 to run RIP v2 as the routing protocol to exchange the loopback networks. FW Access-list outside permit udp host 10.11.11.2 host 224.0.0.9 eq rip Access-list inside permit udp host 10.11.11.1 host 224.0.0.9 eq rip ! Access-group outside in interface outside Access-group inside in interface inside R1 Router RIP No auto-summary Version 2 Net 10.0.0.0 R2 Router RIP No auto-summary Version 2 Net 10.0.0.0 Task 2 Allow R1 to Telnet and HTTP into R2. FW Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 213 of 404 Access-list inside permit tcp host 10.11.11.1 host 10.11.11.2 eq 23 Access-list inside permit tcp host 10.11.11.1 host 10.11.11.2 eq 80 Task 3 The devices on the inside of the Firewall should be able to go out for Web, SMTP and DNS traffic only. FW Access-list inside permit tcp any any eq 80 Access-list inside permit tcp any any eq 21 Access-list inside permit udp any any eq 53 Task 4 You will be configuring MPLS-Unicast Routing on R1 and R2 in the future. Make sure the Firewall allows them to communicate to each other. Also, allow BPDU packets and packets with a EtherType 0x2111 thru the Firewall. FW access-list E-TYPE ethertype permit bpdu access-list E-TYPE ethertype permit mpls-unicast access-list E-TYPE ethertype permit 0x2111 access-group E-TYPE in interface inside access-group E-TYPE in interface outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 214 of 404 Lab 4 – Configuring NAT on a Transparent Firewall Lab Scenario: Configure NAT on a Transparent Firewall. Initial Setup: Based on the previous Lab Task 1 Create a loopback 100 on R1. Assign it an address of 10.111.111.111/24. Configure the Firewall with a static route for this network. The Firewall should translate all traffic going from this network towards outside using a pool of 192.1.20.151-192.1.20.199. Back this pool up by using a PAT address of 192.1.20.200. Create a static route for 192.1.20.0/24 network on R2 & R3 pointing towards the appropriate next hop. This network was assigned to the company as the public range. FW Route inside 10.111.111.0 255.255.255.0 10.11.11.1 ! object network POOL-10-1 range 192.1.20.151 192.1.20.199 ! object network POOL-P-10-1 host 192.1.20.200 ! object-group network NAT-PAT-10-1 network-object object POOL-10-1 network-object object POOL-P-10-1 ! object network NET-10-1 subnet 10.111.111.0 255.255.255.0 nat (inside,outside) dynamic NAT-PAT-10-1 R1 Interface Loopback 100 Ip address 10.111.111.111 255.255.255.0 R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 215 of 404 Ip route 192.1.20.0 255.255.255.0 192.1.23.2 R2 Ip route 192.1.20.0 255.255.255.0 10.11.11.10 Task 2 There is a Web server located at 10.111.111.25. This server should be seen as 192.1.20.151 on the Internet. Perform the translation on the Firewall. R1 should be seen as 192.1.20.1 on the Internet. Allow access to these devices from the Internet. FW object network S1-WWW host 10.111.111.25 nat (ins,outside) static 192.1.20.151 ! object network R1 host 10.1.1.1 nat (ins,outside) static 192.1.20.1 ! Access-list OUTSIDE permit tcp any host 10.1.1.1 eq 23 Access-list OUTSIDE permit tcp any host 10.111.111.25 eq 80 ! Access-group OUTSIDE in interface outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 216 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 6: Configuring the Firewall Component of FTD Module 6 – Configuring the Firewall Component of FTD Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 217 of 404 Lab 1 – Initial Configuration of Firepower Threat Defence [FTD] & FMC from CLI R 1 MGMT PC F 0/0 (.1) 10.11.11.0/24 ASA E0/1 (.10) 192.168.3.0/24 192.168.1.0/24 E0/2 (.10) (.46) F0/0 (.3) R3 (.45) E0/0 (.10) 192.1.20.0/24 FMC F 0/0 (.2) R2 Lab Scenario: Initializing the Management parameters of the FTD Device from CLI. Initial Setup: Configure the IP Addresses based on the Diagram. Configure the following Static Routes on the appropriate routers: o o o o Default Default Default Default Routes on R1 pointing towards 10.11.11.10. Route on the FW towards 192.1.20.2. Route on R3 towards 192.1.20.10. Routes on R2 pointing towards 192.168.3.0/24 Configure the following Loopback addresses on R1,R2 & R3: o R1 : 10.1.1.0/24, 100.1.1.1/2 o R2 : 2.2.2.0/24,199.1.1.1/24,200.1.1.1/24 o R3 : 10.3.3.0/24 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 218 of 404 R1 R2 Int Loopback 1 Ip add 10.1.1.1 255.255.255.0 ! Int loopback 100 Ip add 100.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.10 Int Loopback 1 Ip add 2.2.2.2 255.255.255.0 ! Int loopback 199 Ip add 199.1.1.1 255.255.255.0 ! Int Loopback 200 Ip add 200.1.1.1 255.255.255.0 ! Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.20.10 R3 Int Loopback 1 Ip add 10.3.3.3 255.255.255.0 ! Int F 0/0 Ip add 192.168.3.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.168.3.10 Lab Tasks: Task 1 1. Configure an IP address on the FTD as 192.168.1.46/24 with a Default Gateway of 192.168.1.1. FTD CLI configure network ipv4 manual 192.168.1.46 255.255.255.0 192.168.1.1 Task 2 Configure the Firepower Management Center [FMC] IP as 192.168.1.45/24 with a default gateway of 192.168.1.1. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 219 of 404 FMC CLI configure-network Do you wish to Configure iPv4? [y or n] y Management IP Address>?[] 192.168.1.45 Management netmask?[] 255.255.255.0 Management default gateway? [] 192.168.1.1 Management IP address? Management netmask? Management default gateway? 192.168.1.45 255.255.255.0 192.168.1.1 Are these settings correct? (y or n) y Do you wish to configure IPv6 (y or n) n Wait for it to complete the configuration. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 220 of 404 Lab 2 – Registering & Initializing the FTD Device on FMC Lab Scenario: Configure the FTD to use the FMC as the Manager Device from CLI Register the FTD in the FMC Console. Configure the Intial Setup of FTD. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the address for the Management FMC along with a secret key of cisco123 FTD CLI configure manager add 192.168.1.45 cisco123 Task 2 Log into the FMC using a browser [Use IE]The default username is Admin generally with a password of Sourcefire or Admin123 PC Solution of AVI Task 3 Register the FTD. Create a Default Policy that will Block all the Traffic. PC Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 221 of 404 Task 4 Set the Time to be synchronized locally: PC System -> configuration -> time Synchronization: Set it to locally and save Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 222 of 404 Lab 3 – FTD Interface Configuration Lab Scenario: Configure & Initialize the Interfaces on FTD Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure the FTD with the following IP configuration for the Interfaces: Interface G 0/0 G 0/1 G 0/2 Name Outside Inside DMZ3 Zone OUTSIDE INSIDE DMZ IP Address 192.1.20.10/24 10.11.11.10/24 192.168.3.10/24 At this point, the FTD should be reachable from R1,R2 & R3. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Interfaces Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 223 of 404 Lab 4 – Routing Protocol Configuration – Static and Default Routes Lab Scenario: Configure Default and Static routes on FTD to provide connectivity. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the FTD with a Static Route to the internal loopback network 100.1.1.0/24. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Routing Click Static Routes Click Add Routes Solution on AVI file Task 2 Configure a default route on the FTD pointing towards R2. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Routing Click Static Routes Click Add Routes Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 224 of 404 Lab 5 – Routing Protocol Configuration - Running RIP V2 Lab Scenario: Configure RIP v2 on the Firewall. Configure MD5 authentication for RIP. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure RIP v2 on the FTD on the DMZ interface. Disable autosummarization of routes. Also, configure RIP v2 on R3. Advertise the Loopback network on R3 under RIP. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Routing Click RIP Click to Enable RIP Solution on AVI file R3 Router rip No auto-summary Version 2 Network 192.168.3.0 Network 10.0.0.0 Task 2 Configure the FTD & R3 with RIP v2 authentication using a Key 1 and password of cciesec. FTD [FMC] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 225 of 404 Solution on AVI file R3 Key chain AUTH Key 1 Key-string cciesec ! Int F 0/0 Ip rip authentication mode md5 Ip rip authentication key-chain AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 226 of 404 Lab 6 – Routing Protocol Configuration – Running OSPF Lab Scenario: Configure OSPF on the Firewall. Configure MD5 authentication for OSPF. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure OSPF on the Inside interface of the FTD in Area 0. Hard-code the Router-id as 10.10.10.10. Also, configure OSPF on R1. Hard-code the router-id as 0.0.0.1. Have R1 advertise the Loopback network 10.1.1.0/24 in OSPF. Have the FTD inject a default route towards the Inside network. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Routing Click OSPF Click to Enable OSPF Process 1 Solution on AVI file R1 Router OSPF 1 Router-id 0.0.0.1 Network 10.11.11.0 0.0.0.255 area 0 Network 10.1.1.0 0.0.0.255 area 0 Task 2 Configure the Firewall and R2 with a key of 1 and a password of cciesec. For MD5 authentication. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 227 of 404 FTD [FMC] Solution on AVI file R1 Interface F 0/0 ip Ospf authentication message-digest ip Ospf message-digeset-key 1 md5 cciesec Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 228 of 404 Lab 7 – Routing Protocol Configuration – Running BGP Lab Scenario: Configure BGP on FTD. Configure MD5 authentication for FTD. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure EIGRP on the inside interface of the Firewall in AS 65001 to exchange routes with R2.. Advertise the R2 Loopbacks in BGP. FTD [FMC] Device -> Device Management -> FTD -> Edit [Pencil] -> Routing Click BGP Solution on AVI file R2 Router BGP 65001 Network 2.0.0.0 Network 199.1.1.0 Network 200.1.1.0 Neighbor 192.1.20.10 remote-as 65001 Task 2 Configure the FTD and R2 with BGP authentication using a Key of cciesec. FTD [FMC] Solution on AVI file R2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 229 of 404 Router BGP 65001 Neighbor 192.1.20.10 password cciesec Task 3 Perform Route Redistribution such that all devices have a complete picture of the entire topology. FTD [FMC] Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 230 of 404 Lab 8 – Configuring Access Control Policies – Basic Filtering Lab Scenario: Configure Access Control Policies on the FTD using FMC Console. Configure ACP Policies based on L3 & L4 characteristics. Initial Setup: Based on the previous Lab Lab Task: Task 1 Allow access to the following servers for the specific ports specified below: 192.168.1.11 -> [Web Services – 80 & 443] 192.168.1.12 -> [E-Mail Services – 25] 192.168.1.13 -> [DNS – 53] 192.168.1.3 -> [Telnet & SSH – 22 & 23] 192.168.1.4 -> [TACACS+ - 49] 100.1.1.1 -> [DB Access : 1521] FTD [FMC] Solution on AVI file Task 2 Allow access to the following servers for the specific ports specified below: 192.168.1.21 -> [E-Mail Services – 25] 192.168.1.22 -> [Web Services – 80 & 443] FTD [FMC] Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 231 of 404 Lab 9 – Configuring Access Control Policies – Advanced Filtering Lab Scenario: Configure Access Control Policies on the FTD using FMC Console. Configure ACP Policies based on L3 & L4 characteristics. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Blacklist all Bogon Networks on the Outside Zone. Also, blacklist RFC-1918 address on the Outside Zone. Also, Blacklist Bogon URLs on the Outside Zone. FTD [FMC] Solution on AVI file Task 2 Block all traffic coming in from the Outside zone that is sourced from Russia. Make it a Mandatory rule. FTD [FMC] Solution on AVI file Task 3 Block all High & Medium Risk applications. This should be applied to traffic from INSIDE to OUTSIDE Zones. Make it a Mandatory Rule. FTD [FMC] Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 232 of 404 Task 4 Add a rule at the top of Default Category to block the following URL Categories. This should be done for Traffic from the INSIDE zone to the OUTSIDE zone: Adult & Pornography Gambling Keyloggers & Monitoring FTD [FMC] Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 233 of 404 Lab 10 – Configuring Dynamic NAT & Dyanmic PAT Lab Scenario: Configure Dynamic NAT Configure Dynamic PAT Initial Setup: Based on the previous Lab Lab Task: Task 1 The Firewall should translate all traffic going from 10.11.11.0/24 towards the outside using a pool of 192.1.20.151 – 192.1.20.200. FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Task 2 The Firewall should translate all traffic going from 10.1.1.0/24 towards the outside using an IP Address of 192.1.20.9. FW FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 234 of 404 Lab 11 – Configuring Static NAT & Static Identity NAT Lab Scenario: Configure Static NAT Configure Static Identity NAT Initial Setup: Based on the previous Lab Lab Task: Task 1 Statically translate the following devices on the Outside: 192.168.1.11 192.168.1.12 192.168.1.13 192.168.1.3 192.168.1.4 -> -> -> -> -> 192.1.20.51 [WWW1] 192.1.20.52 [E-MAIL] 192.1.20.53 [DNS] 192.1.20.3 [R3] 192.1.20.54 [ACS] FW FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Task 2 Statically translate R1-Loopback100 [100.1.1.1/32] such that it is seen as itself on the outside. It should not get translated. FW FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 235 of 404 Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 236 of 404 Lab 12 – Configuring Static PAT Lab Scenario: Configure OSPF on the Firewall. Configure MD5 authentication for OSPF. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure Static PAT on the Firewall such that if a request comes from the outside destined for an IP Address 192.1.20.7 with a port number 25, the firewall should forward the request to a SMTP server located at 192.168.3.21 FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Task 2 . If a request comes into the Firewall destined for an IP Address 192.1.20.7 with a port number 80, the Firewall should forward the request to a Device located at 192.168.3.22 for 80. FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 237 of 404 Lab 13 – Configuring Twice-NAT Lab Scenario: Configuring Twice-NAT [Policy NAT] Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall such that when a PC 10.1.1.1 communicates with R2 Loopback199 (199.1.1.1), it is seen as 192.1.20.31 FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Task 2 Configure the Firewall such that when a PC 10.1.1.1 communicates with R2 Loopback200 (200.1.1.1), it is seen as 192.1.20.32. FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 238 of 404 Lab 14 – Configuring Destination NAT Lab Scenario: Configure Destination NAT. Initial Setup: Based on the previous Lab Lab Task: Task 1 There is a Mainframe located on the DMZ at 192.168.3.99. Another Mainframe (200.1.1.1) from the outside needs to access it; The local Mainframe should be seen as 192.1.20.29 on the outside. The local Mainframe does not have the ability to point to a default gateway. Allow the Public Mainframe to access the local Mainframe as a local device located at 192.168.3.98. FTD [FMC] Devices -> NAT -> Create Threat Defence Policy Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 239 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 7: Configuring Intrusion Prevention on FTD Module 7 – Configuring Intrusion Prevention on FTD Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 240 of 404 Lab 1 – Configuring a Balanced Intrusion Policy on FTD Lab Scenario: Configure a Intrusion Policy on FTD Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure an Intrusion Policy using the following parameters: Policy Name: IPS-FTD-POL-1 Drop Mode: Drop Inline Base Policy: Balanced Security & Connectivity FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Task 2 All permit rules in the ACP from the previous labs should be checked against this policy. FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 241 of 404 Lab 2 – Tuning an Existing Signature on the Intrusion Policy Lab Scenario: Enabling existing signatures. Changing the Actions on Signatures. Configuring Event Filters. Initial Setup: Based on the previous Lab Lab Task: Task 1 Tune the IPS-FTD-POL-1 created in the previous Lab to enable the following signatures: Signature : "IMAP login buffer overflow attempt" Signature : ID = 5999 FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Task 2 Change the Action of the IMAP signature enabled in the previous task to Generate Events only. FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 242 of 404 Task 3 Change the Action of the Skype signature enabled in the previous task to Drop & Generate Events. FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 243 of 404 Lab 3 – Configuring an Event Filter Lab Scenario: Configuring an Event filter to Bypass a signature Initial Setup: Based on the previous Lab Lab Task: Task 1 The Skype signature enabled in the previous task should not fire for 192.168.1.11 & 10.11.11.1 IP addressess FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 244 of 404 Lab 4 – Configuring a Custom Signature Lab Scenario: Configuring a Custom IPS Signature Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a signature to fire based on a ICMP Packet. FTD [FMC] Objects -> Intrustion Prevention Solution on AVI file Task 2 Enable the Custom Signature in the IPS-FTD-POL-1 policy. It should drop the packet and Generate an event. FTD [FMC] Policies -> Access Control -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 245 of 404 Lab 5 – Configuring a Network Discovery Policy Lab Scenario: Configuring a Network Discovery Policy Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a Network Discovery Policy to discover the Hosts & their applications. The Network Discovery should only be done on the INSIDE and DMZ zones. FTD [FMC] Policies -> Network Discovery Solution on AVI file Task 2 Delete any other policy except for the one that you created in the previous task. FTD [FMC] Policies -> Network Discovery Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 246 of 404 Lab 6 – Configuring an Intrusion Policy based on the Firepower Recommendations Lab Scenario: Configuring the IPS Policy to use Firepower recommendations based on the Network Discovery policy Initial Setup: Based on the previous Lab Lab Task: Task 1 Re-Configure the IPS-FTD-POL-1 policy to include Firepower recommendations. FTD [FMC] Policies -> Intrusion Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 247 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 8: Configuring AMP on FTD Module 8 – Configuring AMP on FTD Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 248 of 404 Lab 1 – Configuring AMP to Block Specific File Types Lab Scenario: Configuring the AMP File Policy to block File Types Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a File & Malware Policy called INSIDE-FILE-POLICY to using the following requirements: Download of any Executable using any protocol – Block. Download of any Archive using HTTP – Block with Reset. Upload of any Executable or Archive Files using any protocol – Block with Reset. Upload of any .MDB file - Block FTD [FMC] Policies -> Malware & File Analysis Solution on AVI file Task 2 Configure a File & Malware Policy called DMZ-FILE-POLICY to using the following requirements: Upload of any Executable or Archive Files using any protocol – Block with Reset. Upload of any .MDB file - Block FTD [FMC] Policies -> Malware & File Analysis Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 249 of 404 Solution on AVI file Task 3 Configure all the Permit policies from INSIDE towards the OUTSIDE zone to check the INSIDE-FILE-POLICY. FTD [FMC] Policies -> Access Control Solution on AVI file Task 4 Configure all the Permit policies from OUTSIDE towards the DMZ zone to check the DMZ-FILE-POLICY. FTD [FMC] Policies -> Access Control Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 250 of 404 Lab 2 – Configure AMP Policies to Block Files Infected with Malware Lab Scenario: Configure AMP Policies for Malware Analysis. Initial Setup: Based on the previous Lab Lab Task: Task 1 Re-configure INSIDE-FILE-POLICY requirements: AMP Policy to using the following Download of any PDF using any protocol – Block Malware with Reset. Check using Dynamic & Local Malware Analysis. Download of any Office Document using any protocol – Block Malware with Reset. Check using Local Malware Anaylysis only. FTD [FMC] Policies -> Access Control Solution on AVI file Task 2 Re-configure DMZ-FILE-POLICY requirements: AMP Policy to using the following Download of any File except for MDB, Executable or Archive files – Block Malware with Reset. Check using Dynamic & Local Malware Analysis. FTD [FMC] Policies -> Access Control Solution on AVI file Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 251 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 9: Configuring Zone-based Firewalls Module 9 – Configuring Zone-based Firewalls Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 252 of 404 Lab1– Configuring Zone-based Firewall on a Router R1 S 0/0 (.1) 192.1.12.0/24 R4 S 0/0 (.2) F 0/0 (.4) F 0/1 (.2) 192.1.24.0/24 R2 F 0/0 (.2) 192.1.23.0/24 F 0/0 (.3) R3 Lab Scenario: Configure R2 as a Zone-Based Firewall to control traffic into the Internal and DMZ Segment. R1 is acting as the Internet. 192.1.23.0/24 is the Internal Network and the 192.1.24.0/24 is the DMZ network. Initial Setup: Configure the IP Addresses based on the Diagram. Configure the 4.2.2.2/24 address on R1. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 253 of 404 Configure the following static and default routes: o Static routes on R1 for the 192.1.23.0/24 and 192.1.24.0/24 networks pointing to R2 as the Next-hop. o Default routes on R3 & R4 pointing towards R2. o Default route on R2 point towards R1. R1 R2 Int loopback 0 Ip add 4.2.2.2 255.255.255.0 ! Int S 0/0 Ip add 192.1.12.1 255.255.255.0 Clock rate 128000 No shut R3 Int S 0/0 Ip add 192.1.12.2 255.255.255.0 No shut ! Int F 0/0 Ip address 192.1.23.2 255.255.255.0 No shut ! Int F 0/1 Ip address 192.1.24.2 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.12.1 R4 Int F 0/0 Ip address 192.1.23.3 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.23.3 Int F 0/0 Ip address 192.1.24.4 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.24.4 Ip route 192.1.23.0 255.255.255.0 192.1.12.2 Ip route 192.1.24.0 255.255.255.0 192.1.12.2 Lab Tasks: Task 1 Configure the zones and apply them based on the following on R2: LOCAL : Interface F 0/0 DMZ : Interface F 0/1 INTERNET : Interface S 0/0 R2 Zone security LOCAL Zone security DMZ Zone security INTERNET ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 254 of 404 Interface S0/0 Zone-member security INTERNET ! Interface F0/0 Zone-member security LOCAL ! Interface F0/1 Zone-member security DMZ Task 2 Allow the Following protocols to go from the LOCAL to the INTERNET zone: HTTP HTTPS DNS FTP TFTP SMTP ICMP RDP R2 Class-map type inspect match-any CM-L-I Match protocol HTTP Match protocol HTTPS Match protocol DNS Match protocol FTP Match protocol TFTP Match protocol SMTP Match protocol ICMP ! policy-map type inspect PM-L-I class type inspect CM-L-I inspect ! Zone-pair security L-I source LOCAL destination INTERNET Service-policy type inspect PM-L-I Task 3 Allow the Following protocols to go from the LOCAL to the DMZ zone: HTTP HTTPS DNS SMTP ICMP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 255 of 404 TELNET R2 Class-map type inspect match-any CM-L-D Match protocol HTTP Match protocol HTTPS Match protocol DNS Match protocol SMTP Match protocol ICMP Match protocol TELNET ! policy-map type inspect PM-L-D class type inspect CM-L-D inspect ! Zone-pair security L-D source LOCAL destination DMZ Service-policy type inspect PM-L-D Task 4 Allow the Following protocols to go from the INTERNET to the DMZ zone: Allow SMTP Access to a server 192.1.24.51 located on the DMZ zone Allow Telnet Access to a router 192.1.24.4 located on the DMZ zone. Only allow R1 to make this connection. R2 Access-list 142 permit ip any host 192.1.24.51 Access-list 143 permit ip host 192.1.12.1 host 192.1.24.4 ! Class-map type inspect match-all CM-I-D-MAIL Access-group 142 Match protocol SMTP ! Class-map type inspect match-all CM-I-D-TELNET Access-group 143 Match protocol TELNET ! Policy-map type inspect PM-I-D Class type inspect CM-I-D-WEB Inspect Class type inspect CM-I-D-MAIL Inspect Class type inspect CM-I-D-TELNET Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 256 of 404 Inspect ! zone-pair security I-D source INTERNET destination DMZ service-policy type inspect PM-I-D Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 257 of 404 Lab 2 – Configuring Port-Maps in Zone-based Network Diagram 1.2 Firewall Lab Scenario: Configure Port-maps to allow port/protocols not natively controlled thru Zone-based Firewall. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure Inspection of RDP from LOCAL to DMZ zone. R2 ip port-map user-RDP port tcp 3389 ! Class-map type inspect CM-L-D Match protocol user-RDP ! Note: No need to call this Class-map in the policy-map as it is already done in the previous lab. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 258 of 404 Lab 3 – Configuring Nested Classes in Zone-based Network Diagram 1.2 Firewalls Lab Scenario: Configuring Nested Classes for advanced configurations. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure Access to a server located at 192.1.24.11 for Web Services [HTTP or HTTPS] R2 Access-list 141 permit ip any host 192.1.24.11 ! Class-map type inspect match-any CM-WEB Match protocol http Match protocol https ! Class-map type inspect match-all CM-I-D-WEB Match class-map CM-WEB Match access-group 141 ! Policy-map type inspect PM-I-D Class CM-I-D-WEB Inspect Note: No need to apply this Policy-map as it is already applied in Lab 1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 259 of 404 CCIE Security v5 – Configuring ASA, FTD, Intrusion Prevention & AMP Module 10 – Configuring VPNs on ASA & FTD Module 10 – Configuring VPNs on ASA & FTD Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 260 of 404 Lab 1 – Configuring LAN-TO-LAN IPSec VPN on ASA – Router - IKEv1 R1 F 0/0 (.1) 10.11.11.0/24 VLAN 11 G 0/1 (.11) FTD G 0/0 (.11) 192.1.10.0/24 R2 F 0/0.1(.5) F 0/0 (.2) R5 F 0/0.2 (.5) F 0/0.4(.5) 192.1.40.0/24 192.1.20.0/24 F 0/0.5(.5) F 0/0.3(.5) F 0/0.6(.5) Test PC (.15) 192.1.41.0/24 192.1.30.0/24 192.1.42.0/24 G 0/0 (.11) G 0/0 (.11) R3 F 0/0 (.3) ASA-2 ASA-1 G 0/1 (.12) G 0/1 (.11) 10.40.40.0/24 VLAN 40 F 0/0 (.4) R4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 261 of 404 Lab Scenario: Configure a LAN-TO-LAN IPSec VPN using IKEv1. Initial Setup: Configure the IP Addresses on the Routers & FW based on the Diagram. Configure the 2 switches to trunk using dot1q. Configure SW1 as the VTP Server in domain cisco. Configure SW2 as the VTP Client in domain cisco. Configure all the VLANs required on SW1. Assign the devices to the appropriate VLANs. Point all the Device to the logical next hop for the Default Gateway. R1 R2 Int F 0/0 Ip add 10.11.11.1 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 10.11.11.11 Int F 0/0 Ip add 192.1.20.2 255.255.255.0 No shut ! Int Loopback0 Ip address 10.2.2.2 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.1.20.5 R4 R3 Int F 0/0 Ip add 192.1.30.3 255.255.255.0 No shut ! Int Loopback0 Ip address 10.3.3.3 255.255.255.0 ! Ip route 0.0.0.0 0.0.0.0 192.1.30.5 Int F 0/0 Ip add 10.40.40.4 255.255.255.0 No shut ! Interface loopback 0 Ip address 10.1.1.1 255.255.255.0 Interface loopback11 Ip address 10.11.11.11 255.255.255.0 ! Ip route 10.2.2.0 255.255.255.0 10.40.40.11 Ip route 10.3.3.0 255.255.255.0 10.40.40.12 R3 FTD Int F 0/0 Interface G 0/0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 262 of 404 No shut ! Int F 0/0.1 Encap vlan 10 Ip add 192.1.10.5 No shut ! Int F 0/0.2 Encap vlan 20 Ip add 192.1.20.5 No shut ! Int F 0/0.3 Encap vlan 30 Ip add 192.1.30.5 No shut ! Int F 0/0.4 Encap vlan 40 Ip add 192.1.40.5 No shut ! Int F 0/0.5 Encap vlan 41 Ip add 192.1.41.5 No shut ! Int F 0/0.6 Encap vlan 40 Ip add 192.1.42.5 No shut SW1 Nameif outside Zone OUTSIDE Ip add 192.1.10.11 255.255.255.0 No shut 255.255.255.0 255.255.255.0 ! Interface G 0/1 Nameif Inside Zone INSIDE Ip add 10.11.11.11 255.255.255.0 No shut ! Default Route: 192.1.10.5 255.255.255.0 255.255.255.0 255.255.255.0 255.255.255.0 Interface range F 0/21 – 22 Swithcport trunk encapsulation dot1q Switchport mode trunk ! Vtp mode server Vtp domain cisco ! Vlan 10 Vlan 11 Vlan 20 Vlan 30 Vlan 40 SW2 Interface range F 0/21 – 22 Swithcport trunk encapsulation dot1q Switchport mode trunk ! Vtp mode client Vtp domain cisco Note : Port Assignment based on the Physical Topology Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 263 of 404 Vlan 41 Vlan 42 Note : Port Assignment based on the Physical Topology ASA1 ASA2 Interface G 0/0 Nameif Outside Ip add 192.1.41.11 255.255.255.0 No shut ! Interface G 0/1 Nameif Inside Ip add 10.40.40.11 255.255.255.0 No shut ! route Outside 0.0.0.0 0.0.0.0 192.1.41.5 route inside 10.1.1.0 255.255.255.0 10.40.40.4 route inside 10.11.11.0 255.255.255.0 10.40.40.4 Interface G 0/0 Nameif Outside Ip add 192.1.42.11 255.255.255.0 No shut ! Interface G 0/1 Nameif Inside Ip add 10.40.40.12 255.255.255.0 No shut ! route Outside 0.0.0.0 0.0.0.0 192.1.41.5 route inside 10.1.1.0 255.255.255.0 10.40.40.4 route inside 10.11.11.0 255.255.255.0 10.40.40.4 Lab Tasks: Task 1 Configure an IPSec Tunnel on ASA1 to encrypt traffic from 10.40.40.0/24 to the 10.2.2.0/24 on R2 (Loopback 0) using the following parameters for IPSec: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : MD5 o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC ASA-1 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 264 of 404 Encryption 3des ! tunnel-group 192.1.20.2 type ipsec-l2l tunnel-group 192.1.20.2 ipsec-attributes pre-shared-key cisco ! crypto ipsec transform-set T-SET esp-3des esp-sha-hmac ! access-list 150 permit ip 10.40.40.0 0.0.0.255 10.2.2.0 0.0.0.255 ! crypto map I-MAP 10 set peer 192.1.40.4 crypto map I-MAP 10 set peer 192.1.40.4 crypto map I-MAP 10 set transform-set T-SET crypto map I-MAP 10 match address 150 ! Crypto map I-MAP Interface Outside R2 Crypto isakmp policy 10 Authentication pre-share Hash md5 Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.41.11 ! crypto ipsec transform-set T-SET esp-3des esp-sha-hmac ! access-list 150 permit ip 10.2.2.0 0.0.0.255 10.40.40.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp set peer 192.1.41.11 set transform-set T-SET match address 150 ! Interface F 0/0 Crypto map I-MAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 265 of 404 Lab 2 – Configuring LAN-TO-LAN IPSec VPN on ASA – Router – IKEv2 Lab Scenario: Configure a LAN-TO-LAN IPSec VPN using IKEv2. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure an IPSec Tunnel on ASA-2 to encrypt traffic from 10.40.40.0/24 to the 10.3.3.0/24 on R3 (Loopback 0) using the following parameters for IPSec: IKEv2 Parameters o Authentication : Pre-shared o Encryption : AES-256 o Group : 2 o Inegrity : SHA-256 o PRF : SHA-256 o Pre-Shared Key : ASA-2-R3 -> cisco11 o Pre-Shared Key : R3-ASA-2 -> cisco22 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC ASA-2 crypto ikev2 policy 17 encryption aes-256 integrity sha256 group 2 prf sha256 lifetime seconds 36000 ! tunnel-group 192.1.30.3 type ipsec-l2l tunnel-group 192.1.30.3 ipsec-attributes Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 266 of 404 ikev2 remote-authentication pre-shared-key cisco11 ikev2 local-authentication pre-shared-key cisco22 ! crypto ipsec ikev2 ipsec-proposal T-SET protocol esp encryption aes-256 protocol esp integrity sha-1 ! access-list 153 extended permit ip 10.40.40.0 255.255.255.0 10.3.3.0 255.255.255.0 ! crypto map I-MAP 10 set peer 192.1.30.3 crypto map I-MAP 10 set ikev2 ipsec-proposal T-SET crypto map I-MAP 10 match address ASA3-R6 crypto map I-MAP interface Outside ! crypto ikev2 enable Outside R3 crypto ikev2 proposal PROP-1 encryption aes-cbc-256 integrity sha256 group 2 ! crypto ikev2 policy POL-1 proposal PROP-1 ! crypto ikev2 keyring KR-1 peer ASA-2 address 192.1.42.11 pre-shared-key local cisco22 pre-shared-key remote cisco11 ! crypto ikev2 profile PROF-1 match identity remote address 192.1.42.11 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR-1 ! crypto ipsec transform-set T-SET esp-aes 256 esp-sha-hmac mode tunnel ! Access-list 150 permit ip 10.3.3.0 0.0.0.255 10.40.40.0 0.0.0.255 ! crypto map I-MAP 10 ipsec-isakmp Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 267 of 404 set peer 192.1.42.11 set transform-set T-SET set ikev2-profile PROF-1 match address 150 ! interface F 0/0 crypto map I-MAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 268 of 404 Lab 3 – Configuring Remote-Access VPN using IPSec on ASA Lab Scenario: Configure a Remote-Access VPN using IPSec with an AnyConnect Client. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure ASA2 as a Local Trustpoint using the information below. Self enroll the certificate. FQDN : ASA2.khawarb.com Trustpoint Name: LOCAL Subject name=ASA2.khawarb.com Key Pair name=VPN ASA-2 domain-name khawarb.com hostname ASA2 ! crypto key generate rsa label VPN modulus 1024 noconfirm ! crypto ca trustpoint LOCAL enrollment self fqdn ASA2.khawarb.com subject-name CN=ASA2.khawarb.com keypair VPN ! crypto ca enroll LOCAL noconfirm Task 2 Configure the IKEv2 Profile file as an XML file called IKEv2.xml and upload the file to ASA-2. The content of the XML is give below. ASA-2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 269 of 404 Solution of AVI File Task 3 Enable Webvpn on the ASA2. Use the anyconnect file on flash as the image file. Enable webvn such that the client have the ability to pick the Tunnel group. Use the anyconnect profile created in the previous Task. Name the Profile as IKEv2. ASA-2 webvpn enable outside anyconnect image disk0:/anyconnect-win-4.2.01022-k9.pkg anyconnect enable tunnel-group-list enable anyconnect profiles IKEv2 flash:IKEv2.xml Solution of AVI File Task 4 Configure the Group Policies using the following information: Group ADMINS o VPN-Tunnel-Protocol : IKEv2 o DNS Server: 8.8.8.8 o Anyconnect profile : IKEv2 Group EMPLOYEES o VPN-Tunnel-Protocol : IKEv2 o DNS Server: 8.8.8.8 o Anyconnect profile : IKEv2 ASA-2 group-policy ADMINS internal group-policy ADMINS attributes vpn-tunnel-protocol IKEv2 dns-server value 8.8.8.8 webvpn anyconnect profiles value IKEv2 type user ! group-policy EMPLOYEES internal group-policy EMPLOYEES attributes vpn-tunnel-protocol IKEv2 dns-server value 8.8.8.8 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 270 of 404 webvpn anyconnect profiles value IKEv2 type user Task 5 Configure the Tunnel-group Policies using the following information: Tunnel-Group ADMINS o Default-group-policy : ADMINS o Group-Alias: ADMINS o VPN Pool – ADMINS : 192.168.51.1 192.168.51.254 Tunnel-Group EMPLOYEES o Default-group-policy : EMPLOYEES o Group-Alias: EMPLOYEES o VPN Pool – EMPLOYEES : 192.168.52.1 192.168.52.254 ASA-2 ip local pool ADMINS 192.168.51.1-192.168.51.254 mask 255.255.255.0 ! tunnel-group ADMINS type remote-access tunnel-group ADMINS general-attributes address-pool ADMINS default-group-policy ADMINS ! tunnel-group ADMINS webvpn-attributes group-alias ADMINS enable ! ip local pool EMPLOYEES 192.168.52.1-192.168.52.254 mask 255.255.255.0 ! tunnel-group EMPLOYEES type remote-access tunnel-group EMPLOYEES general-attributes address-pool EMPLOYEES default-group-policy EMPLOYEES ! tunnel-group EMPLOYEES webvpn-attributes group-alias EMPLOYEES enable Task 6 Configure the Usernames based on the following: username Khawar password Cisco123 username John password Cisco123 ASA-2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 271 of 404 username Khawar password Cisco123 username John password Cisco123 Task 7 Configure IKEv2 & IPSec Policies using the information below Trustpoint : LOCAL SSL Trustpoint Interface : Outside username John password Cisco123 IKEv2 Policy: o Encryption: 3Des o Integrity & PRF: SHA1 o Group: 2 IPSec Policy: o Encryption: 3Des o Integrity & PRF: SHA1 ASA-2 crypto ikev2 enable outside client-services 443 crypto ikev2 remote-access trustpoint LOCAL ssl trust-point LOCAL outside ! crypto ikev2 policy 10 encryption aes group 2 5 ! crypto ipsec ikev2 ipsec-proposal ABC protocol esp encryption 3des protocol esp integrity SHA-1 Task 8 Configure a Dynamic Map and link it to a Static Map. Configure reverse-route. Apply the Map to the Outside Interface. ASA-2 crypto dynamic-map DMAP 10 set ikev2 ipsec-proposal ABC crypto dynamic-map DMAP 10 set reverse-route ! Crypto map ABC 65000 ipsec-isakmp dynamic DMAP ! crypto map ABC interface Outside Task 9 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 272 of 404 Browse to the Outside Interface IP address of ASA-2 using https. Download & Install the client. Use the client to establish a IKEv2 VPN to the ASA network. TEST PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 273 of 404 Lab 4 – Configuring Remote-Access VPN using SSL on ASA Lab Scenario: Configure a Remote-Access VPN using SSL with an AnyConnect Client. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Enable Webvpn on the ASA1. Use the anyconnect file on flash as the image file. Enable webvn such that the client have the ability to pick the Tunnel group. ASA1 webvpn enable outside anyconnect image disk0:/anyconnect-win-4.2.01022-k9.pkg anyconnect enable tunnel-group-list enable Task 2 Configure the Group Policies & the VPN Pool using the following information: Group ADMINS o Split-tunnel networks: 10.1.1.0/24 & 10.11.11.0/24 o VPN-Tunnel-Protocol : SSL-Client Group EMPLOYEES o Split-tunnel networks: 10.11.11.0/24 o VPN-Tunnel-Protocol : SSL-Client ASA1 access-list ADMINS standard permit 10.1.1.0 255.255.255.0 access-list ADMINS standard permit 10.11.11.0 255.255.255.0 ! group-policy ADMINS internal group-policy ADMINS attributes vpn-tunnel-protocol ssl-client Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 274 of 404 split-tunnel-policy tunnelspecified split-tunnel-network-list value ADMINS ! ! access-list EMPLOYEES standard permit 10.11.11.0 255.255.255.0 ! group-policy EMPLOYEES internal group-policy EMPLOYEES attributes vpn-tunnel-protocol ssl-client split-tunnel-policy tunnelspecified split-tunnel-network-list value EMPLOYEES Task 3 Configure the Tunnel-group Policies using the following information: Tunnel-Group ADMINS o Default-group-policy : ADMINS o Group-Alias: ADMINS o VPN Pool – ADMINS : 192.168.51.1 192.168.51.254 Tunnel-Group EMPLOYEES o Default-group-policy : EMPLOYEES o Group-Alias: EMPLOYEES o VPN Pool – EMPLOYEES : 192.168.52.1 192.168.52.254 ASA1 ip local pool ADMINS 192.168.51.1-192.168.51.254 mask 255.255.255.0 ! tunnel-group ADMINS type remote-access tunnel-group ADMINS general-attributes address-pool ADMINS default-group-policy ADMINS ! tunnel-group ADMINS webvpn-attributes group-alias ADMINS enable ! ! ip local pool EMPLOYEES 192.168.52.1-192.168.52.254 mask 255.255.255.0 ! tunnel-group EMPLOYEES type remote-access tunnel-group EMPLOYEES general-attributes address-pool EMPLOYEES default-group-policy EMPLOYEES ! tunnel-group EMPLOYEES webvpn-attributes Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 275 of 404 group-alias EMPLOYEES enable Task 4 Configure the Usernames based on the following: username Khawar password Cisco123 username John password Cisco123 ASA1 username Khawar password Cisco123 username John password Cisco123 Task 5 Browse to the Outside Interface IP address of ASA-1 using https. Download & Install the client. Use the client to establish a SSL VPN to the ASA network. TEST PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 276 of 404 Lab 5 – Configuring Clientless SSL VPN on ASA Lab Scenario: Configure a Remote-Access VPN using Clientless SSL VPN. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure ASA2 for Clientless WebVPN using the following Parameters: Group: SALES o VPN-Tunnel-Protoco: SSL-Clientless o Banner : Authorized Users Only !!! o Port-forward: SALES-APPS 30001:10.11.11.1:80 30002:10.11.11.1:23 30003:10.11.11.1:1521 Users: o Jane – Password – Cisco123 o Group-policy - SALES ASA2 WebVPN - Basic webvpn enable outside port-forward SALES-APPS 30001 10.11.11.1 80 port-forward SALES-APPS 30002 10.11.11.1 23 port-forward SALES-APPS 30003 10.11.11.2 1521 ! group-policy SALES internal group-policy SALES attributes vpn-tunnel-protocol ssl-clientless banner value "XXXX" webvpn port-forward value SALES-APPS Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 277 of 404 ! username khawar password cisco123 username khawar attributes vpn-group-policy SALES Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 278 of 404 Lab 6 – Configuring IPSec LAN-TO-LAN VPN on FTD – IKEv1 Lab Scenario: Configure a LAN-TO-LAN IPSec VPN from FTD to a Router using IKEv1. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure an IPSec Tunnel to encrypt traffic from 10.11.11.0/24 behind FTD to the 10.2.2.0/24 on R2 (Loopback 0) using the following parameters for IPSec: ISAKMP Parameters o Authentication : Pre-shared o Encryption : 3DES o Group : 2 o Hash : SHA o Pre-Shared Key : cisco IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC FTD [FMC] Solution on AVI file R2 Crypto isakmp policy 20 Authentication pre-share Hash SHA Group 2 Encryption 3des ! Crypto isakmp key cisco address 192.1.10.11 ! Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 279 of 404 crypto ipsec transform-set T-SET esp-3des esp-sha-hmac ! access-list 151 permit ip 10.2.2.0 0.0.0.255 10.11.11.0 0.0.0.255 ! crypto map I-MAP 20 ipsec-isakmp set peer 192.1.10.11 set transform-set T-SET match address 151 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 280 of 404 Lab 7 – Configuring IPSec LAN-TO-LAN VPN on FTD – IKEv2 Lab Scenario: Configure a LAN-TO-LAN IPSec VPN from FTD to a Router using IKEv2. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure an IPSec Tunnel on FTD to encrypt traffic from 10.11.11.0/24 to the 10.3.3.0/24 on R3 (Loopback 0) using the following parameters for IPSec: IKEv2 Parameters o Authentication : Pre-shared o Encryption : AES-256 o Group : 2 o Inegrity : SHA-256 o PRF : SHA-256 o Pre-Shared Key : FTD-R3 -> cisco11 o Pre-Shared Key : R3-FTD -> cisco22 IPSec Parameters o Encryption : ESP-3DES o Authentication : ESP-SHA-HMAC FTD [FMC] Solution on AVI file R3 crypto ikev2 keyring KR-1 peer FTD address 192.1.10.11 pre-shared-key local cisco22 pre-shared-key remote cisco11 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 281 of 404 ! crypto ikev2 profile PROF-2 match identity remote address 192.1.10.11 255.255.255.255 authentication remote pre-share authentication local pre-share keyring local KR-1 ! Access-list 151 permit ip 10.3.3.0 0.0.0.255 10.11.11.0 0.0.0.255 ! crypto map I-MAP 20 ipsec-isakmp set peer 192.1.10.11 set transform-set T-SET set ikev2-profile PROF-2 match address 151 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 282 of 404 CCIE Security v5 – Configuring ACS 5.X for AAA Module 1 – Configuring ACS for Management Authentication Module 1 – Configuring Management Authentication Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 283 of 404 ACS for Lab 1 – Configuring a Router to Authenticate Using the ACS Server Cisco ACS Server SW1 R5 F 0/0 (.5) (.15) 192.1.10.0/24 VLAN 10 E 0/1 (.10) ASA (.25) F 0/1 (.1) R1 F 0/0 (.3) R3 F 0/1 (.3) E 0/0 (.10) 192.1.20.0/24 VLAN 20 192.1.34.0/24 VLAN 34 F 0/0 (.2) F 0/0 (.4) R2 R4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 284 of 404 Lab Scenario: Configure the Router to communicate to the ACS server using TACACS or RADIUS as the authentication protocol. Authenticate Telnet & SSH connections based on the ACS using Local Username database as the backup authentication mechanism. Initial Setup: Configure the IP Addresses on the Routers & FW based on the Diagram. R1 R2 Int F 0/0 Ip add 192.168.43.1 255.255.255.0 No shut Int F 0/0 Ip add 192.168.43.2 255.255.255.0 No shut R3 SW1 Int F 0/0 Ip add 192.168.43.3 255.255.255.0 No shut Int vlan 10 Ip address 192.168.43.15 255.255.255.0 No shut FW Interface G 0/1 Nameif inside Ip add 192.168.43.10 255.255.255.0 No shut Lab Tasks: Task 1 Configure R1 and R2 as clients to the ACS Server. R1 should use TACACS+ as the authentication protocol and R2 should use RADIUS as the authentication protocol. Both should use ccie-r as the secret key. ACS Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 285 of 404 Task 2 Configure a group called R-Admins on the ACS . ACS Solution on AVI File Task 3 Create the following users and make them members of the R-Admin group: Username – Ruser1 Password: ruser1 Username – Ruser2 Password: ruser2 Username – Ruser3 Password: ruser3 ACS Solution on AVI File Task 4 Configure R1 and R2 to communicate with the ACS server for authentication. Use the key and address in Task 1. R1 Aaa new-model Tacacs-server host 192.1.10.25 key ccie-r ** do test aaa group tacacs ruser1 ruser1 legacy. ** This command verifies that the ACS is communicating to the device R2 Aaa new-model radius-server host 192.1.10.25 key ccie-r ** do test aaa group radius ruser1 ruser1 legacy ** This command verifies that the ACS is communicating to the device Task 5 Configure Telnet and SSH Authentication to be done based on the ACS server for R1 & R2. If the ACS server is not available, they should use the Local database for authentication. Create a user on the router called admin with a password of admin. Make sure the Console port is

not authenticated R1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 286 of 404 Username admin password admin ! Ip domain-name abc.com Crypto key generate rsa ! Aaa authentication login T-AUTH group tacacs local Aaa authentication login NO-AUTH none ! line vty 0 4 login authentication T-AUTH ! line console 0 login authentication NO-AUTH R2 Username admin password admin ! Ip domain-name abc.com Crypto key generate rsa ! Aaa authentication login R-AUTH group radius local Aaa authentication login NO-AUTH none ! line vty 0 4 login authentication R-AUTH ! line console 0 login authentication NO-AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 287 of 404 Lab 2 – Configuring a Switch to Authenticate Using the ACS Server Lab Scenario: Configure a Switch to communicate to the ACS server using RADIUS as the authentication protocol. Authenticate Telnet based on the ACS using Local Username database as the backup authentication mechanism. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure SW1 as a client to the ACS Server. SW1 should use RADIUS as the authentication protocol. Use ccie-sw as the secret key. ACS Solution on AVI File Task 2 Configure a group called SW-Admins. ACS Solution on AVI File Task 3 Create the following users and make them members of the SW-Admin group: Username – swuser1 Password: swuser1 Username – swuser2 Password: swuser2 Username – swuser3 Password: swuser3 ACS Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 288 of 404 Task 4 Configure SW1 to communicate with the ACS server for authentication. Use the key and address in Task 1. SW1 Aaa new-model radius-server host 192.1.10.25 key ccie-sw ** do test aaa group radius swuser1 swuser1 legacy. ** This command verifies that the ACS is communicating to the device Task 5 Configure Telnet Authentication to be done based on the ACS server for SW1. If the ACS server is not available, it should use the Local database for authentication. Create a user on the switch called admin with a password of admin. Make sure the Console port is not authenticated SW1 Username admin password admin ! Aaa authentication login R-AUTH group radius local Aaa authentication login NO-AUTH none ! line vty 0 4 login authentication R-AUTH ! line console 0 login authentication NO-AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 289 of 404 Lab 3 – Configuring a Firewall to Authenticate Using the ACS Server Lab Scenario: Configure a Firewall to communicate to the ACS server using TACACS as the authentication protocol. Authenticate Telnet & SSH connections based on the ACS using Local Username database as the backup authentication mechanism. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure the Firewall as a client to the ACS Server. The Firewall should use TACACS+ as the authentication protocol. It should use ccie-fw as the secret key. ACS Solution on AVI File Task 2 Configure a group called FW-Admins. ACS Solution on AVI File Task 3 Create the following users and make them members of the FW-Admin group: Username – fwuser1 Password: fwuser1 Username – fwuser2 Password: fwuser2 Username – fwuser3 Password: fwuser3 ACS Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 290 of 404 Solution on AVI File Task 4 Configure the Firewall to communicate with the ACS server for authentication. Use the key and address in Task 1. FW Aaa-server ACS protocol tacacs Aaa-server ACS host 192.1.10.25 Key ccie-fw ** do test aaa authentication ACS host 192.1.10.25 ** This command verifies that the ACS is communicating to the device Task 5 Configure the Firewall for SSH. Configure SSH & Telnet Authentication to be done based on the ACS server. If the ACS server is not available, the Firewall should use the Local database for authentication. Create a user on the Firewall called admin with a password of admin. FW Username admin password admin ! domain-name abc.com Crypto key generate rsa ! Aaa authentication ssh console ACS LOCAL Aaa authentication telnet console ACS LOCAL Task 6 Allow Telnet from the 192.1.10.0 subnet only. Allow SSH from the 192.1.10.0/24 and 192.1.20.0/24 subnets. FW telnet 192.1.10.0 255.255.255.0 inside ssh 192.1.10.0 255.255.255.0 inside ssh 192.1.20.0 255.255.255.0 outside Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 291 of 404 CCIE Security v5 – Configuring ACS 5.X for AAA Module 2 – Configuring ACS for Management Authorization Module 2 – Configuring Management Authorization Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 292 of 404 ACS for Lab 1 – Configuring a Router for Exec Authorization Using the ACS Cisco ACS Server SW1 R5 F 0/0 (.5) (.15) 192.1.10.0/24 VLAN 10 E 0/1 (.10) ASA (.25) F 0/1 (.1) R1 F 0/0 (.3) R3 F 0/1 (.3) E 0/0 (.10) 192.1.20.0/24 VLAN 20 192.1.34.0/24 VLAN 34 F 0/0 (.2) F 0/0 (.4) R2 R4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 293 of 404 Lab Scenario: Configuring a Custom Privilege Level on a Router that restricts a user to a limited set of commands. Configure the Router to use the ACS server to assign the Privilege levels to the user. Initial Setup: Based on the previous Lab Lab Task: Task 1 Ruser1 and Ruser2 should be assigned Privilege Level 15 by the ACS server. ACS Solution on AVI File Task 2 Configure R1 to perform Exec authorization on the VTY lines based on the ACS server. R1 aaa authorization exec T-AUTH group tacacs+ ! line vty 0 4 authorization exec T-AUTHOR Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 294 of 404 Lab 2 – Configuring a Router for Command Authorization Using the ACS Lab Scenario: Configuring the Router to perform Login Authentication, Authorization and Command Authorization against the ACS Server. Exec Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R5 as client to the ACS Server. R5 should use TACACS+ as the authentication protocol. It should use ccie-r as the secret key. ACS Solution on AVI File Task 2 Configure R5 to communicate with the ACS server for authentication. Use the key and address in Task 1. R5 Aaa new-model Tacacs-server host 192.1.10.25 key ccie-r ** do test aaa group tacacs ruser1 ruser1 legacy. ** This command verifies that the ACS is communicating to the device Task 3 Configure R5 to perform VTY authentication, Exec Authorization and Command Authorization for Level 15 commands based on the ACS Server. Assign all the users to Privilege level 15. They should be able to execute commands in Privilege Exec and Global Configuration modes based on Command Authorization from the ACS Server. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 295 of 404 R5 Aaa authentication login T-AUTH group tacacs Aaa authorization exec T-AUTH group tacacs Aaa authorization command 15 T-AUTH group tacacs Aaa authorization config-commands ! Line vty 0 4 Login authentication T-AUTH Authorization exec T-AUTH Authorization command 15 T-AUTH Task 4 Configure 3 Shell Command Authorization sets on the ACS with the following commands and capabilities: RP-ADMIN o Configure terminal o Router RIP (Only allow him to enable RIP as a Routing Protocol) o Execute the Network command for any network o Execute the Version command; Limit it version 2 only o Execute the no auto-summary command SEC-ADMIN o Configure Terminal o Any Crypto command with any Arguments o Authentication command with any Arguments o Encryption command ; Limit it to 3des only o Hash command with any Arguments o Group command ; Limit it to 2 only o Access-list command with any Arguments o set command with any Arguments o match command with any Arguments o Interface command with any Arguments SuperAdmin o Should be allowed all commands. ACS Solution on AVI File Task 5 Assign the Shell Command Authorization Sets to the Users based on the following: Ruser1 – SuperAdmin Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 296 of 404 Ruser2 – RP-ADMIN Ruser3 – SEC-ADMIN ACS Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 297 of 404 Lab 3 – Configuring ACS Authentication for HTTP Management on a Router Lab Scenario: Configuring a Router for HTTP Management. Authenticating and Authorizing the HTTP Management based on the ACS Server. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R5 to allow HTTP Management. It should only allow HTTP Management from VLAN 10. R5 access-list 15 permit 192.1.10.0 0.0.0.255 ! ip http server ip http access-class 15 Task 2 Authenticate and Authorize the users connecting into R5 for HTTP using the authentication and authorization lists configured in the previous Lab. R5 ip http authentication aaa login-authentication T-AUTH ip http authentication aaa exec-authorization T-AUTH ip http authentication aaa command-authorization 15 T-AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 298 of 404 CCIE Security v5 – Configuring ACS 5.X for AAA Module 3 – Configuring ACS for Management Accounting Module 3 – Configuring Management Accounting Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 299 of 404 ACS for Lab 1 – Configuring Exec and Command Accounting on a Router Cisco ACS Server SW1 R5 F 0/0 (.5) (.15) 192.1.10.0/24 VLAN 10 E 0/1 (.10) ASA (.25) F 0/1 (.1) R1 F 0/0 (.3) R3 F 0/1 (.3) E 0/0 (.10) 192.1.20.0/24 VLAN 20 192.1.34.0/24 VLAN 34 F 0/0 (.4) R2 R4 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 300 of 404 Lab Scenario: Configure the Routers to log all Telnet and SSH connections to the ACS Server. Configure Routers to log commands typed in by Administrators while logged in to the ACS. Initial Setup: Based on the previous Lab Lab Task: Task 1 Track logins and logouts thru telnet & SSH into R1 & R5 to the ACS Server. R1 aaa accounting exec T-ACCT start-stop group tacacs+ ! line vty 0 4 accounting exec T-ACCT R5 aaa accounting exec T-ACCT start-stop group tacacs+ ! line vty 0 4 accounting exec T-ACCT Task 2 Log all Level 15 commands typed by these users while logged in thru telnet & SSH. R1 aaa accounting commands 15 T-ACCT start-stop group tacacs+ ! line vty 0 4 accounting commands 15 T-ACCT R5 aaa accounting commands 15 T-ACCT start-stop group tacacs+ Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 301 of 404 ! line vty 0 4 accounting commands 15 T-ACCT Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 302 of 404 Lab 2 – Configuring Exec Accounting on a Switch Lab Scenario: Configure the Switch to log all Telnet and SSH connections to the ACS Server. Initial Setup: Based on the previous Lab Lab Task: Task 1 Track logins and logouts thru telnet & SSH into the Switch to the ACS Server. SW1 aaa accounting exec R-ACCT start-stop group radius ! line vty 0 4 accounting exec R-ACCT Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 303 of 404 Lab 3 – Configuring Telnet & SSH connection Accounting Lab Scenario: Configure the Firewall to log all Telnet and SSH connections to the ACS Server. Initial Setup: Based on the previous Lab Lab Task: Task 1 Track logins and logouts thru telnet & SSH into the Firewall to the ACS Server. FW Aaa accounting telnet console ACS Aaa accounting ssh console ACS Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 304 of 404 CCIE Security v5 – Configuring WLC & WAP Module 1 – Initial Configuration of the WLC & WAP Module 1 – Initial Configuration of the Wireless LAN Controller (WLC) & the Wireless Access Point (WAP) Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 305 of 404 Lab 1 – Basic Intialization of the Wireless LAN Controller (WLC) 192.168.20.0/24 VLAN 20 192.168.30.0/24 VLAN 30 R2 R3 F 0/0 (.3) F 0/0 (.2) 192.168.10.0/24 VLAN 10 F 0/1 (.1) R1 E 0/0 (.1) WiFi Enabled PC 192.168.100.0/24 VLAN 100 (.100) (.50) PC WLC WAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 306 of 404 Lab Scenario: Initialize the Wireless Controller. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure the VLANs on the switches based on your physical setup to match the Logical setup in the diagram. Run EIGRP in AS 100 on the Routers to have complete routing in the network. Configure R1 with the local time zone and time. Configure R1 as a NTP Master with a stratum of 2. R1 R2 Int F 0/0 Ip add 192.168.123.1 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.10.1 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.168.123.0 Network 192.168.10.0 ! Clock timezone IST 5 30 Do clock set 12:30:00 1 February 2013 ! NTP Master 2 R3 Int F 0/0 Ip add 192.168.10.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.20.2 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.168.20.0 Network 192.168.10.0 Int F 0/0 Ip add 192.168.10.3 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.30.3 255.255.255.0 PC 1 IP Address : 192.168.123.50 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.123.1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 307 of 404 No shut ! Router eigrp 100 No auto-summary Network 192.168.10.0 Network 192.168.30.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 308 of 404 Lab Tasks: Task 1 Re-initialize the WLC if required by using the Recover-config command from the CLI. WLC Recover-config Task 2 Initialize the WLC based on the following parameters: Hostname : WLC Admin Username : admin Admin Password : Cisco123 IP Address : 192.168.123.99 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.123.1 Management VLAN : 123 Physical Interface : 1 Virtual-IP : 100.100.100.100 Mobility Group : MGMT Management SSID : MGMT Country : ES Radio : Enable all Radio Auto RF : Yes NTP Server : NO Manual Time: Set it based on the Current time. WLC Solution on AVI File Task 3 Open a browser. Type . Login using the administrator name and password created in the previous step. Are you successful?? WLC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 309 of 404 Lab 2 – Basic Configuration of the Wireless Access Point (WAP) Using DHCP Lab Scenario: Configure R1 as the DHCP Server to give out IP Address for VLAN 100. All the AP's will be located on this segment. Make sure the WAP communicates and registers with the WLC. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R1 as the DHCP Server for VLAN 100. It should be configured with the following parameters: DHCP Pool Name : VLAN123 DHCP Range to be used : 192.168.123.101 – 192.168.100.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.123.1 WLC Address : 192.168.123.99 R1 IP DHCP excluded-address 192.168.123.1 192.168.123.100 ! IP DHCP Pool VLAN100 Network 192.168.123.0 /24 Default-router 192.168.123.1 Option 43 ip 192.168.123.99 Task 2 Configure R1 as the DHCP Server for VLAN 10. It should be configured with the following parameters: DHCP Pool Name : VLAN10 DHCP Range to be used : 192.168.10.101 – 192.168.10.254 DHCP Subnet : 255.255.255.0 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 310 of 404 Default Router : 192.168.10.1 R1 IP DHCP excluded-address 192.168.10.1 192.168.10.100 ! IP DHCP Pool VLAN10 Network 192.168.10.0 /24 Default-router 192.168.10.1 Task 3 Configure R1 as the DHCP Server for VLAN 20. It should be configured with the following parameters: DHCP Pool Name : VLAN20 DHCP Range to be used : 192.168.20.101 – 192.168.20.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.20.2 R1 IP DHCP excluded-address 192.168.20.1 192.168.20.100 ! IP DHCP Pool VLAN20 Network 192.168.20.0 /24 Default-router 192.168.20.2 Task 4 Configure R1 as the DHCP Server for VLAN 30. It should be configured with the following parameters: DHCP Pool Name : VLAN30 DHCP Range to be used : 192.168.30.101 – 192.168.30.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.30.3 R1 IP DHCP excluded-address 192.168.30.1 192.168.30.100 ! IP DHCP Pool VLAN30 Network 192.168.30.0 /24 Default-router 192.168.30.3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 311 of 404 Task 3 Make sure that the WAP has registered with the WLC. WLC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: b.com Page 312 of 404 CCIE Security v5 – Configuring WLC & WAP Module 2 – Configuring a Basic Wireless LAN Module 2 – Wireless LAN Configuring Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 313 of 404 a Basic Lab 1 – Creating VLAN Interface on the WLC Lab Scenario: Configuring VLAN Interfaces for different VLANs. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a VLAN Interface for VLAN 10 based on the following parameters: Interface Name : VLAN10 VLAN : 10 Physical Interface : 2 IP Configuration o IP Address : 192.168.10.100 o Subnet : 255.255.255.0 o Default Gateway : 192.168.10.1 DHCP Server : 192.168.100.1 WLC Solution on AVI File Task 2 Configure a VLAN Interface for VLAN 20 based on the following parameters: Interface Name : VLAN20 VLAN : 20 Physical Interface : 2 IP Configuration o IP Address : 192.168.20.100 o Subnet : 255.255.255.0 o Default Gateway : 192.168.20.2 DHCP Server : 192.168.100.1 WLC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 314 of 404 Task 3 Configure a VLAN Interface for VLAN 30 based on the following parameters: Interface Name : VLAN30 VLAN : 30 Physical Interface : 2 IP Configuration o IP Address : 192.168.30.100 o Subnet : 255.255.255.0 o Default Gateway : 192.168.30.3 DHCP Server : 192.168.100.1 WLC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 315 of 404 Lab 2 – Configuring WLANs, SSIDs and Associating them with VLAN Interfaces – Open Authentication Lab Scenario: Configuring a WLAN with Open Authentication Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a WLAN for the SALES VLAN (20) using the following parameters: WLAN Name : SALES SSID : SALES Interface : VLAN20 Security : Open WLC Solution on AVI File Task 2 Go to Network Connections; Right-click on the Wireless NIC; Click View Wireless Networks; Select SALES. Did you connect? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 316 of 404 Task 3 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 4 Open the Command prompt. Type tracert 192.168.30.3. What are the hops from the Wireless client to the destination? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 317 of 404 Lab 3 – Configuring WLANs, SSIDs and Associating them with VLAN Interfaces – Static WEP PSK (40-Bit) Lab Scenario: Configuring a WLAN with Static WEP – PSK (40-bit) Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a WLAN for the Marketing VLAN (30) using the following parameters: WLAN Name : MARKETING SSID : MARKETING Interface : VLAN30 Security : Static WEP o PSK : 40-bit – C1SCO WLC Solution on AVI File Task 2 Go to Network Connections; Right-click on the Wireless NIC; Click View Wireless Networks; Select MARKETING. When prompted, type the PSK configured in the previous step.. Did you connect? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 318 of 404 Task 3 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 4 Open the Command prompt. Type tracert 192.168.20.2. What are the hops from the Wireless client to the destination? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 319 of 404 Lab 4 – Configuring WLANs, SSIDs and Associating them with VLAN Interfaces – Static WEP PSK (104-Bit) Lab Scenario: Configuring a WLAN with Static WEP – PSK (104-bit) Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a WLAN for the IT VLAN (10) using the following parameters: WLAN Name : IT SSID : IT Interface : VLAN10 Security : Static WEP o PSK : 104-bit – C1SCOcisco123 WLC Solution on AVI File Task 2 Go to Network Connections; Right-click on the Wireless NIC; Click View Wireless Networks; Select IT. Did you connect? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 320 of 404 Task 3 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 4 Type tracert 192.168.20.2. What are the hops from the Wireless client to the destination? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 321 of 404 Lab 5 – Configuring SSID's with Web Authentication Lab Scenario: Configuring SSID with Web Authentication. Initial Setup: Based on the previous Lab Lab Task: Task 1 Change the configuration of the IT WLAN to also ask for Web Authentication. WLC Solution on AVI File Task 2 Configure a local user with the following attributes: Username : Khawar Password : ccie12353 Allowed WLAN : IT WLC Solution on AVI File Task 3 Go to Network Connections; Right-click on the Wireless NIC; Click View Wireless Networks; Select IT. Did you connect? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 322 of 404 Task 4 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 5 Ping 192.168.10.1. Are you able to ping your default gateway? Why or Why not? PC Solution on AVI File Task 6 Open your browser and browse to . Does it ask for Web Authentication? Type the Username credentials created in Task 2. Is the authentication successful? PC Solution on AVI File Task 6 Ping 192.168.10.1. Are you able to ping your default gateway? Why or Why not? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 323 of 404 CCIE Security v5 – Configuring ISE for Wired & Wireless Authentication & Posture Validation Module 1 – Configuring ISE to Communicate to the Switch & WLC Network Devices Module 1 – Configuring ISE to Communicate to the Switch & WLC Network Devices Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 324 of 404 Lab 1 – Preparing the Network for ISE R4 192.168.20.0/24 VLAN 20 192.168.30.0/24 VLAN 30 F 0/0 (.4) 192.1.40.0/24 VLAN 40 G 0/0 (.10) F 0/1 (.3) F 0/1 (.2) R3 R2 G 0/1(.10) F 0/0(.3) F 0/0 (.2) 192.168.10.0/24 VLAN 10 F 0/1 (.10) SW1 SW2 R1 F 0/0 (.1) WiFi Enabled PC (.15) (.16) 192.168.123.0/24 VLAN 123 (.35) ISE (.100) (.50) PC WLC WAP Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 325 of 404 Lab Scenario: Configuring the Network for ISE Deployment. Initial Setup: Configure the IP Addresses on the Routers based on the Diagram. Configure the VLANs on the switches based on your physical setup to match the Logical setup in the diagram. Run EIGRP in AS 100 on the Routers to have complete routing in the network. Configure R1 with the local time zone and time. Configure R1 as a NTP Master with a stratum of 2. R1 R2 Int F 0/0 Ip add 192.168.123.1 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.10.1 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.168.123.0 Network 192.168.10.0 ! Clock timezone IST 5 30 Do clock set 12:30:00 1 February 2013 ! NTP Master 2 R3 Int F 0/0 Ip add 192.168.10.2 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.20.2 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.168.20.0 Network 192.168.10.0 Int F 0/0 Ip add 192.168.10.3 255.255.255.0 No shut ! Int F 0/1 Ip add 192.168.30.3 255.255.255.0 PC 1 IP Address : 192.168.123.50 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.123.1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 326 of 404 No shut ! Router eigrp 100 No auto-summary Network 192.168.10.0 Network 192.168.30.0 R4 Int F 0/0 Ip add 192.1.40.4 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.1.40.0 ! Line vty 0 4 Password cisco login ASA Int G 0/0 Nameif Outside Ip add 192.1.40.10 255.255.255.0 No shut ! Int G 0/1 Nameif Inside Ip add 192.168.10.10 255.255.255.0 No shut ! Router eigrp 100 No auto-summary Network 192.168.10.0 Network 192.1.40.0 Lab Tasks: Task 1 Configure R1 as a DNS Server. It should resolve the following domain-names to the IP: Ise.abc.in : 192.168.123.254 R1.abc.in : 192.168.123.1 R1 IP DNS Server ! IP host ise.ABC.in 192.168.123.35 IP host R1.ABC.in 192.168.123.1 Task 2 Configure R1 as the DHCP Server for VLAN 123. It should be configured with the following parameters: DHCP Pool Name : VLAN123 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 327 of 404   DHCP Range to be used : 192.168.123.101 – 192.168.123.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.123.1 DNS Server : 192.168.123.1 WLC Address : 192.168.123.99 R1 IP DHCP excluded-address 192.168.123.1 192.168.123.100 ! IP DHCP Pool VLAN123 Network 192.168.123.0 /24 Default-router 192.168.123.1 Dns-Server 192.168.123.1 Option 43 ip 192.168.123.99 Task 3 Configure R1 as the DHCP Server for VLAN 10. It should be configured with the following parameters: DHCP Pool Name : VLAN10 DHCP Range to be used : 192.168.10.101 – 192.168.10.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.10.1 DNS Server : 192.168.100.1 R1 IP DHCP excluded-address 192.168.10.1 192.168.10.100 ! IP DHCP Pool VLAN10 Network 192.168.10.0 /24 Default-router 192.168.10.10 Dns-Server 192.168.100.1 Task 4 Configure R1 as the DHCP Server for VLAN 20. It should be configured with the following parameters: DHCP Pool Name : VLAN20 DHCP Range to be used : 192.168.20.101 – 192.168.20.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.20.2 DNS Server : 192.168.100.1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 328 of 404 R1 IP DHCP excluded-address 192.168.20.1 192.168.20.100 ! IP DHCP Pool VLAN20 Network 192.168.20.0 /24 Default-router 192.168.20.2 Dns-Server 192.168.100.1 Task 5 Configure R1 as the DHCP Server for VLAN 30. It should be configured with the following parameters: DHCP Pool Name : VLAN30 DHCP Range to be used : 192.168.30.101 – 192.168.30.254 DHCP Subnet : 255.255.255.0 Default Router : 192.168.30.3 DNS Server : 192.168.100.1 R1 IP DHCP excluded-address 192.168.30.1 192.168.30.100 ! IP DHCP Pool VLAN30 Network 192.168.30.0 /24 Default-router 192.168.30.3 Dns-server 192.168.100.1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 329 of 404 Lab 2 – Basic Intialization of Identity Service Engine (ISE) Lab Scenario: Initializing the ISE Creating Endpoint Identity Groups Creating User Identity Groups Configuring Profiling Creating Users Update the Posture Database Initial Setup: Based on the previous Lab Lab Task: Task 1 Open a Browser and browse to . The Username of the the ISE is admin. The Password was set to ISE Solution on AVI File Task 2 Change the Deployment Mode to Primary. ISE Solution on AVI File Task 3 Update the Posture Database based on the offline method. The File for the posture update should be located in the LabFiles Folder. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 330 of 404 ISE Solution on AVI File Task 4 Turn on Profiling on the ISE appliance for the following probes: DHCP DHCP SPAN RADIUS ISE Solution on AVI File Task 5 Configure the following Endpoint & User Identity Groups on the ISE appliance: ADMIN-PC – Endpoint Identity Group SALES – User Identity Group MARK – User Identity Group IT – User Identity Group Physical PC – Endpoint Identity Group ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 331 of 404 Lab 3 – Associating the Switch with the ISE Appliance Lab Scenario: Configure the 2 Switches to communicate to the ACS server using RADIUS as the authentication protocol. Initial Setup: Based on the previous Lab Lab Task: Task 1 Open the ISE Admin page and configure the SW1 as a Network Device using cisco123 as the secret key. ISE Solution on AVI File Task 2 Open the ISE Admin page and configure the SW1 as a Network Device using cisco123 as the secret key. ISE Solution on AVI File Task 3 Configure SW1 to communicate to ISE using RADIUS as the protocol and cisco123 as the secret key. Also, configure the Switches with a local username of admin with a password of admin. Configure a enable password of cisco. This will be used by the ISE to Validate the Config for ISE. SW1 Aaa new-model Radius-server host 192.168.123.35 key cisco123 ! Username admin privilege 15 password admin Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 332 of 404 Enable secret cisco Task 4 Configure SW2 to communicate to ISE using RADIUS as the protocol and cisco123 as the secret key. Also, configure the Switches with a local username of admin with a password of admin. Configure a enable password of cisco. This will be used by the ISE to Validate the Config for ISE. SW2 Aaa new-model Radius-server host 192.168.123.35key cisco123 ! Username admin password admin Enable secret cisco Task 5 Use the Config Validation Operation Tool to telnet into SW1 and validate the config. All the configuration that appears in red needs to be filled up. Use notepad to do that and paste the config to SW1. Optionally, you can use the Dot1x Switch config file that I have provided in the Labfiles folder. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 333 of 404 Lab 4 – Initializing & Associating the WLC with the ISE Appliance Lab Scenario: Initializing the WLC thru the CLI. Configure the WLC to communicate to the ACS server using RADIUS as the authentication protocol. Initial Setup: Based on the previous Lab Lab Task: Task 1 Re-initialize the WLC if required by using the Recover-config command from the CLI. WLC Recover-config Task 2 Initialize the WLC based on the following parameters: Hostname : WLC Admin Username : admin Admin Password : Cisco123 IP Address : 192.168.123.99 Subnet Mask : 255.255.255.0 Default Gateway : 192.168.123.1 Management VLAN : 123 Physical Interface : 1 Virtual-IP : 100.100.100.100 Mobility Group : MGMT Management SSID : MGMT Radio : Enable all Radio Auto RF : Yes NTP Server : N Manual : Set it based on Local Time Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 334 of 404 WLC Solution on AVI File Task 3 Open a browser. Type . Login using the administrator name and password created in the previous step. Are you successful?? WLC Solution on AVI File Task 4 In WLC, under the Security Menu, configure the WLC to communicate to ISE (192.168.123.35) as the authentication and accounting server. Use cisco123 as the secret key. WLC Solution on AVI File Task 5 Open the ISE Admin page and configure the WLC as a Network Device using cisco123 as the secret key. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 335 of 404 CCIE Security v5 – Configuring ISE for Wired & Wireless Authentication & Posture Validation Module 2 – Configuring 802.1x Using ISE Module 2 – Configuring 802.1x Using ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 336 of 404 Lab 1 – Configuring 802.1x Authentication for a Wired Client Lab Scenario: Configuring ISE to authenticate Wired Clients for 802.1x Authentication. Configure the Windows client to support Dot1x Authentication Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Default Network Policy Results for authentication to support MSCHAP v2. Also, completely disable EAP-TLS for the policy (3 locations). ISE Solution on AVI File Task 2 Configure the following User Identities and assign them to the appropriate groups: Username : Sales1 – Password : Cisco123 – Group : Sales Username : Mark1 – Password : Cisco123 – Group : Mark Username : IT1 – Password : Cisco123 – Group : IT ISE Solution on AVI File Task 3 Under the Authentication page, Change the name of Dot1x Authentication to Dot1x_Wired. Don't change any other property. Save the Configuration change. ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 337 of 404 Solution on AVI File Task 4 Run the services.msc file from the Run menu. Make sure the WiredAutoConfig service is running. This turns on the Dot1x service on the PC. PC Solution on AVI File Task 5 On the Wired Dot1x client machine, follow the instructions below to make sure the device is ready for Dot1x authentication.   Open Network and Sharing Center. Click on Adapter Settings. Right-click the LAN adapter and click Properties. Click the Authentication tab. Make sure the Enable IEEE 802.1x Authentication checkbox is selected. Make sure Protected EAP is the authentication Method. Uncheck all the other checkboxes. Click on the Additional settings button. Configure the Authentication Method to User Authentication and click OK. Click on the Settings button. Uncheck all the checkboxes, specifically the Validate Server Certificate. Make sure EAP-MS-CHAP v2 is the authentication Method. Click on the Configure button. Uncheck the "Automatica Logon" checkbox. Click OK all the way to save the configuration. PC Solution on AVI File Task 6 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using Sales1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 338 of 404 Task 7 Open the command prompt. Type IPCONFIG. What IP address was assigned to the User?. It should be from the VLAN that was configured on the Switchport (VLAN 100). PC Solution on AVI File Task 8 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. SW2 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 339 of 404 Lab 2 – Configuring 802.1x Authentication for a Wired Client with VLAN Assignment Lab Scenario: Configuring ISE to authorize Wired Clients for 802.1x Authentication for VLAN Assignment Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Authorization Policies Result sets to assign Users to VLANS. Configure the following policies: IT_WIRED_AUTH – VLAN – 10 SALES_WIRED_AUTH – VLAN – 20 MARK_WIRED_AUTH – VLAN – 30 ISE Solution on AVI File Task 2 Configure the Authorization Policies based on the following: Name : IT_DOT1X_WIRED o Group : IT o Authentication Type : Wired_802.1x o Auth. Profile : IT_WIRED_AUTH Name : SALES_DOT1X_WIRED o Group : SALES o Authentication Type : Wired_802.1x o Auth. Profile : SALES_WIRED_AUTH Name : MARK_DOT1X_WIRED o Group : MARK o Authentication Type : Wired_802.1x o Auth. Profile : MARK_WIRED_AUTH Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 340 of 404 ISE Solution on AVI File Task 3 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using IT1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 4 Open the command prompt. Type IPCONFIG. What IP address was assigned to the User?. PC Solution on AVI File Task 5 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. Also, check to see the VLAN assignment to the port. Does it match the running config? SW2 Solution on AVI File Task 6 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using Sales1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 7 Open the command prompt. Type IPCONFIG. What IP address was assigned to the User? PC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 341 of 404 Solution on AVI File Task 8 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. Also, check to see the VLAN assignment to the port. Does it match the running config? SW2 Solution on AVI File Task 9 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using Mark1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 10 Open the command prompt. Type IPCONFIG. What IP address was assigned to the User? PC Solution on AVI File Task 11 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. Also, check to see the VLAN assignment to the port. Does it match the running config? SW2 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 342 of 404 Lab 3 – Configuring 802.1x Authentication for a Wired Client with DACL Assignment Lab Scenario: Configuring ISE to authorize Wired Clients for 802.1x Authentication for DACL Assignment Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Authorization Policies Result DACLs to control User traffic. Configure the following policies: SALES_WIRED_DACL o Deny icmp any host 192.168.123.16 o Permit ip any any MARK_WIRED_DACL o Deny ip any host 192.168.123.16 o Permit ip any any ISE Solution on AVI File Task 2 Configure/modify the Authorization Policies Result sets to control User traffic based on DACL. Configure the following policies: SALES_WIRED_AUTH – VLAN – 20 / DACL – SALES_WIRED_DACL MARK_WIRED_AUTH – VLAN – 30 / DACL – MARK_WIRED_DACL ISE Solution on AVI File Task 3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 343 of 404 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using IT1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 4 Open the command prompt. Type Ping 192.168.123.16. Are you successful? Use Putty to telnet to 192.168.123.16. Are you successful? PC Solution on AVI File Task 5 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. SW2 Solution on AVI File Task 6 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using Sales1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 7 Open the command prompt. Type Ping 192.168.123.16. Are you successful? Use Putty to telnet to 192.168.123.16. Are you successful? PC Solution on AVI File Task 8 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 344 of 404 F X/X to get more detailed information about the authentication. Also, check to see the VLAN & DACL assignment to the port. Does it match the running config? SW2 Solution on AVI File Task 9 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Click on it and Log in using Mark1 as the username with a password of Cisco123. Did you connect?? PC Solution on AVI File Task 10 Open the command prompt. Type Ping 192.168.123.16. Are you successful? Use Putty to telnet to 192.168.123.16. Are you successful? PC Solution on AVI File Task 11 On SW2, type the Show authentication session command to verify the authentication. You can also use the Show authentication session interface F X/X to get more detailed information about the authentication. Also, check to see the VLAN & DACL assignment to the port. Does it match the running config? SW2 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 345 of 404 Lab 4 – Configuring 802.1x Authentication for a Wireless Client with VLAN Assignment Lab Scenario: Configuring the WLC for 802.1x Authentication and VLAN Assignment. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a VLAN Interface for VLAN 10 based on the following parameters: Interface Name : IT VLAN : 10 Physical Interface : 2 IP Configuration o IP Address : 192.168.10.99 o Subnet : 255.255.255.0 o Default Gateway : 192.168.10.10 DHCP Server : 192.168.10.1 WLC Solution on AVI File Task 2 Configure a VLAN Interface for VLAN 20 based on the following parameters: Interface Name : SALES VLAN : 20 Physical Interface : 2 IP Configuration o IP Address : 192.168.20.100 o Subnet : 255.255.255.0 o Default Gateway : 192.168.20.2 DHCP Server : 192.168.123.1 WLC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 346 of 404 Solution on AVI File Task 3 Configure a VLAN Interface for VLAN 30 based on the following parameters: Interface Name : MARK VLAN : 30 Physical Interface : 2 IP Configuration o IP Address : 192.168.30.100 o Subnet : 255.255.255.0 o Default Gateway : 192.168.30.3 DHCP Server : 192.168.123.1 WLC Solution on AVI File Task 4 Configure a common WLAN for company that will use ISE for VLAN and Interface assignment. Configure the WLAN based on the following: WLAN Name : ABC_ISE SSID : ABC_ISE Interface : Management Security : WPA2-Enterprise Settings: o Allow AAA interface override o Authentication & Accounting Servers : 192.168.123.35 o NAC-State o Authentication Order : RADIUS should be preffered WLC Solution on AVI File Task 5 Under the Authentication page, Copy the Dot1x_Wired policy. Set the name of the authentication policy to Dot1x_Wireless. Change the authentication method condition to Wireless_802.1x. Leave the rest of the parameters the same. Save the Policy. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 347 of 404 Task 6 Configure the Authorization Policies Result sets to assign Wireless Users to VLANS. Configure the following policies: IT_WIRELESS_AUTH – VLAN – 10 SALES_WIRELESS_AUTH – VLAN – 20 MARK_WIRELESS_AUTH – VLAN – 30 ISE Solution on AVI File Task 7 Configure the Authorization Policies based on the following: Name : IT_DOT1X_WIRELESS o Group : IT o Authentication Type : Wireless_802.1x o Auth. Profile : IT_WIRELESS_AUTH Name : SALES_DOT1X_WIRELESS o Group : SALES o Authentication Type : Wireless_802.1x o Auth. Profile : SALES_WIRELESS_AUTH Name : MARK_DOT1X_WIRELESS o Group : MARK o Authentication Type : Wireless_802.1x o Auth. Profile : MARK_WIRELESS_AUTH ISE Solution on AVI File Task 8 Go to Network Connections; Right-click on the Wireless NIC; Click View Wireless Networks; Select ABC_ISE. Login in as IT1. Did you connect? PC Solution on AVI File Task 9 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 348 of 404 Solution on AVI File Task 10 Open the Command prompt. Type tracert 192.168.30.3. What are the hops from the Wireless client to the destination? PC Solution on AVI File Task 11 Bounce the Wireless NIC (Disable & Enable it). Right-click on the Wireless NIC; Click View Wireless Networks; Select ABC_ISE. Login in as Sales1. Did you connect? PC Solution on AVI File Task 12 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 13 Open the Command prompt. Type tracert 192.168.30.3. What are the hops from the Wireless client to the destination? PC Solution on AVI File Task 14 Bounce the Wireless NIC (Disable & Enable it). Right-click on the Wireless NIC; Click View Wireless Networks; Select ABC_ISE. Login in as Mark1. Did you connect? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 349 of 404 Task 15 Open a command prompt. Type ipconfig. What IP address was assigned to the wireless client? PC Solution on AVI File Task 16 Open the Command prompt. Type tracert 192.168.20.2. What are the hops from the Wireless client to the destination? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 350 of 404 Lab 5 – Configuring Wired MAB Authentication with VLANAssignment Lab Scenario: Configuring ISE to authenticate Wired Clients for MAB. Initial Setup: Based on the previous Lab Lab Task: Task 1 Under the Authentication page, Change the name of MAB Authentication to MAB_Wired. Don't change any other property. Save the Configuration change. ISE Solution on AVI File Task 2 Open the command prompt on the Wired Client PC. Type IPCONFIG /all. Find out the MAC Address. Copy it into Notepad. Change the format to XX:XX:XX:XX:XX:XX. PC Solution on AVI File Task 3 Add a Endpoint Identity in ISE. Use the MAC Address of the PC. Assign this Endpoint to the ADMIN-PC endpoint group. ISE Solution on AVI File Task 4 Configure the Authorization Policy Result sets to assign the ADMIN_PC Endpoint Group a specific VLAN. Configure the following policy: Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 351 of 404 ADMIN_PC_WIRED_MAB – VLAN – 10 ISE Solution on AVI File Task 5 Configure a new Authorization Policy based on the following: Name : ADMIN_PC_WIRED_MAB o Group : ADMIN_PC o Authentication Type : Wired_MAB o Auth. Profile : ADMIN_PC_WIRED_MAB ISE Solution on AVI File Task 6 Bounce the LAN Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Do NOT put any credentials. Let me fail to MAB. Check the Switch to make sure the Authentication is success based on MAB using the Show authentication session interface F X/X command. PC Solution on AVI File SW1 Solution on AVI File Task 7 Open the command prompt. Type IPCONFIG. What IP address was assigned to the Device? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 352 of 404 Lab 6 – Configuring Wireless MAB Authentication with VLAN Assignment Lab Scenario: Configuring ISE to authenticate Wireless Clients for MAB. Initial Setup: Based on the previous Lab Lab Task: Task 1 Under the Authentication page, copy the MAB_WIRED policy. Change the name to MAB_Wireless. Change the Method to Wireless_MAB. Don't change any other property. Save the Configuration change. ISE Solution on AVI File Task 2 Open the command prompt on the Wireless Client PC. Type IPCONFIG /all. Find out the MAC Address. Copy it into Notepad. Change the format to XX:XX:XX:XX:XX:XX. PC Solution on AVI File Task 3 Add a Endpoint Identity in ISE. Use the MAC Address of the PC. Assign this Endpoint to the ADMIN-PC endpoint group. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 353 of 404 Task 4 Configure the Authorization Policy Result sets to assign the ADMIN_PC Endpoint Group a specific VLAN. Configure the following policy: ADMIN_PC_WIRELESS_MAB – VLAN – 10 ISE Solution on AVI File Task 5 Configure a new Authorization Policy based on the following: Name : ADMIN_PC_WIRELESS_MAB o Group : ADMIN_PC o Authentication Type : Wireless_MAB o Auth. Profile : ADMIN_PC_WIRELESS_MAB ISE Solution on AVI File Task 6 Bounce the Wireless Adapter. (Disable and Enable). A ballon near the system tray will ask ask you for additional credentials. Do NOT put any credentials. Let me fail to MAB. Check the Switch to make sure the Authentication is success based on MAB using the Show authentication session interface F X/X command. PC Solution on AVI File SW1 Solution on AVI File Task 7 Open the command prompt. Type IPCONFIG. What IP address was assigned to the Device? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 354 of 404 Lab 7 – Configuring Wired MAB Authentication for IP Phone & Dot1x for PC behind it Lab Scenario: Configuring ISE to authenticate Cisco IP Phones. Initial Setup: Based on the previous Lab Lab Task: Task 1 Make sure the IP Phone has been profiled as a IP Phone. PC Solution on AVI File SW1 Solution on AVI File Task 7 Open the command prompt. Type IPCONFIG. What IP address was assigned to the Device? PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 355 of 404 CCIE Security v5 – Configuring ISE for Wired & Wireless Authentication & Posture Validation Module 3 – Configuring Posture Validation Using ISE Module 3 – Configuring Validation Using ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 356 of 404 Posture Lab 1 – Configuring Client Provisioning Resources & Policies Lab Scenario: Configure the Client Provisiong Resources for the NAC and Web Agents. Configure Client Provisioning Policy Initial Setup: Based on the previous Lab Lab Task: Task 1 Add the Client files under the Policy Results for Client Provisioning resources. ISE Solution on AVI File Task 2 Configure a Client Provisioning Policy ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 357 of 404 Lab 2 – Configuring Posture Validation based on Operating System & Anti-Virus Requirements Lab Scenario: Configuring Posture Validation with AV and OS Condition Sets Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Policy Condition for Symantec ISE Solution on AVI File Task 2 Configure Posture Validaton for Windows PC based on Any Symantic Anit-virus for the SALES group. ISE Solution on AVI File Task 3 Configure an Authorization Policy Result for the Pre-Auth VLAN with Posture Validation. Configure the ACL on the Switch. ISE Solution on AVI File Task 4 Configure a Authorization policy for Pre-auth based on Compliant and Noncompliant. Assign the Pre-Auth Result ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 358 of 404 Solution on AVI File Task 5 Use the Existing Authorization Profile for SALES and change it to add a session condition of compliant. ISE Solution on AVI File Task 6 Test on PC ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 359 of 404 Lab 3 – Configuring Posture Validation based on Operating System & Application Requirements Lab Scenario: Configuring Posture Validation with AV and Application Condition Sets Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Policy Condition for Notepad under Application Condition ISE Solution on AVI File Task 2 Configure Posture Validaton for Windows PC based on running notepad.exe for the MARK group. ISE Solution on AVI File Task 3 Use the Existing Authorization Profile for MARK and change it to add a session condition of compliant. ISE Solution on AVI File Task 6 Test on PC ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 360 of 404 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 361 of 404 CCIE Security v5 – Configuring ISE for Wired & Wireless Authentication & Posture Validation Module 4 – Configuring CiscoTrust Sec with SGT Exchange Protocol [SXP] Module 4 – Configuring CiscoTrust Sec with SGT Exchange Protocol [SXP] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 362 of 404 Lab 1 – Configuring CTS SXP Relationship between ISE & the WLC & ASA Lab Scenario: Enabling the SXP Service on ISE. Configuring CTS SXP relationship between ISE & WLC Configuring CTS SXP relationship between ISE & ASA Initial Setup: Based on the previous Lab Lab Task: Task 1 Enable SXP Service on ISE. ISE Administration -> System -> Deployment -> Node -> Policy Service -> Enable SXP Service Solution on AVI File Task 2 Configure cisco123 as the Global Password that will be used in the SXP relationships. ISE Work Center -> TrustSec -> Settings -> SXP Settings Global Password : cisco123 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 363 of 404 Task 3 Configure a relationship between the WLC and ISE. WLC should be configured as a speaker and ISE should be configured as a Listener. ISE Work Center -> TrustSec -> SXP -> SXP Devices -> Add Name : WLC IP Address: 192.168.123.99 Peer Role: Speaker Connected PSN : ISE Password : Default Version : v4 Solution on AVI File WLC Security -> TrustSec SXP Select : Enabled Password : cisco123 Apply Click New to add the Peer Peer IP address : 192.168.123.35 Task 4 Configure a relationship between the ASA Firewall and ISE. ASA should be configured as a Listener and ISE should be configured as a Speaker. ISE Work Center -> TrustSec -> SXP -> SXP Devices -> Add Name : ASA IP Address: 192.168.10.10 Peer Role: Listener Connected PSN : ISE Password : Default Version : v4 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 364 of 404 ASA cts sxp enable cts sxp default password cisco123 cts sxp default source-ip 192.168.10.10 cts sxp connection peer 192.168.123.35 password default mode peer speaker Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 365 of 404 Lab 2 – Configuring SGT Group Setup on ISE Lab Scenario: Configuring SGT Configuration settings on ISE Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure SGT Configration settings on ISE based on the following information: Manual SGT Numbering – 6000-6100 Auto Security Group Creation when creating Authorization Rules. o Range – 5000-5100 o Auto - Name – Auhorization Rule Name with a Prefix of SGT. ISE Workcenter -> TrustSec -> Settings -> General TrustSec Settings Security Group Tag Numbering -> User Must Enter SGT Numbers Manually Auto Security Group Creation when creating Authorization Rules Auto SGT Numbers - 5000 - 5100 Auto-Naming Options Solution on AVI File Task 2 Re-create the Wireless Authorization Policies by duplicating them. Copy to Recreate policies for MARK & SALES. It should automatically create the SGTs. Rename the rules to the following: SXP-MARK-WIRELESS. SXP-SALES-WIRELESS. Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 366 of 404 ISE Solution on AVI File Task 3 Delete the Old Wireless Rules. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 367 of 404 Lab 3 – Configuring SGT Based ACL's on the ASA Firewall Lab Scenario: Configure SGT Based ACL's on the ASA Firewall. Verify SXP by logging in from the Wireless Client. Initial Setup: Based on the previous Lab Lab Task: Task 1 Find the SGT Mapping for SALES and MARK Wireless Authorized Users on ISE. ISE Solution on AVI File Task 2 Configure an ACL on the ASA Firewall based on the following information: Sales o o Mark o o Wireless Clients: Allow Telnet to the Outside Allow ICMP to the Outside Wireless Clients: Allow Telnet to the Outside Allow SSH to the Outside ASA Object-group security SGT_SALES_WIRELESS security-group tag 5001 Object-group security SGT_MARK_WIRELESS security-group tag 5002 ! access-list ABC permit tcp object-group-security SGT_SALES_WIRELESS any any eq 23 access-list ABC permit icmp object-group-security SGT_SALES_WIRELESS any any Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 368 of 404 access-list ABC permit tcp object-group-security SGT_MARK_WIRELESS any any eq 23 access-list ABC permit tcp object-group-security SGT_MARK_WIRELESS any any eq 22 ! access-group ABC in interface Inside ! access-list OUTSIDE permit icmp any any echo-reply Access-group OUTSIDE in interface outside Task 3 Test on PC ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 369 of 404 CCIE Security v5 – Configuring ISE for Wired & Wireless Authentication & Posture Validation Module 5 – Configuring ISE for Device Administration Module 1 – Configuring ISE for Device Administration Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 370 of 404 Lab 1 – Configuring a TACACS+ relationship between ISE & Router/Switch Lab Scenario: Configure the Router to communicate to the ISE using TACACS+ for Device Administration. Configure the Router to communicate to the ISE using TACACS+ for Device Administration. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Enable the Device Administration Service on ISE. ISE Solution on AVI File Task 2 Configure R1 and SW2 as clients to the ACS Server. R1 & SW1 should use TACACS+ as the authentication protocol. Both should use cisco123 as the secret key. ISE Solution on AVI File Task 3 Configure the following grousp on ISE: Group Name: Super-Admins Group Name: RP-Admins Group Name: Sec-Admins ISE Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 371 of 404 Solution on AVI File Task 4 Create users on ISE based on the following: Username – Admin1 Password: Admin1 Group: Super-Admins Username – RPadmin1 Password: RPadmin1 Group: RP-Admins Username – SecAdmin1 Password: SecAdmin1 Group: Sec-Admins ISE Solution on AVI File Task 5 Configure R1 and SW2 to communicate with the ACS server for authentication. Use the key and address in Task 1. R1 Aaa new-model Tacacs-server host 192.168.123.35 key cisco123 ** do test aaa group tacacs Admin1 Admin1 legacy. ** This command verifies that the ISE is communicating to the device SW2 Aaa new-model Tacacs-server host 192.168.123.35 key cisco123 ** do test aaa group tacacs Admin1 Admin1 legacy. ** This command verifies that the ISE is communicating to the device Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 372 of 404 Lab 2 – Configuring ISE to support Device Administration Lab Scenario: Configure Privelge Level Policy on ISE. Configure Command Sets on ISE. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure a Shell Profile that assigns a default privilege level of 15. ISE Solution on AVI File Task 2 Configure 3 Shell Command Authorization sets on the ACS with the following commands and capabilities: RP-ADMINS o Configure terminal o Router RIP (Only allow him to enable RIP as a Routing Protocol) o Execute the Network command for any network o Execute the Version command; Limit it version 2 only o Execute the no auto-summary command Sec-ADMINS o Configure Terminal o Any Crypto command with any Arguments o Authentication command with any Arguments o Encryption command ; Limit it to 3des only o Hash command with any Arguments o Group command ; Limit it to 2 only o Access-list command with any Arguments o set command with any Arguments Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 373 of 404 o match command with any Arguments o Interface command with any Arguments Super-Admins o Should be allowed all commands. ISE Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 374 of 404 Lab 3 – Configure the Router & Switch to Use ISE for Authentication & Authorization Lab Scenario: Configure Router/Switch for Authentication. Configure the Router/Switch for Exec and Command Authorization. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure R1 & SW2 to use ISE for login authentication. Create a local username with a username of admin with a password of admin. Assign the local user a privilege levelof 15. Use a Named-list called T-AUTHEN. T-AUTHEN should use the TACACS+ as the primary authentication choice and Local Database for fallback authentication. R1 Username admin privilege 15 password admin ! Aaa authentication login T-AUTHEN group tacacs+ local SW2 Username admin privilege 15 password admin ! Aaa authentication login T-AUTHEN group tacacs+ local Task 2 Configure R1 & SW2 to use ISE for Exec authorization. Use a Named-list called T-AUTHOR. T-AUTHOR should use the TACACS+ as the primary Exec authorization choice and Local Database for fallback authentication. R1 Aaa authorization exec T-AUTHOR group tacacs+ local Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 375 of 404 SW2 Aaa authorization exec T-AUTHOR group tacacs+ local Task 3 Configure R1 & SW2 to use ISE for Command authorization for Level 15 commands. Use a Named-list called T-AUTHOR. T-AUTHOR should use the TACACS+ as the primary authorization choice for Level 15 commands. R1 Aaa authorization command 15 T-AUTHOR group tacacs+ local Aaa authorization config-commands SW2 Aaa authorization command 15 T-AUTHOR group tacacs+ local Aaa authorization config-commands Task 4 Verify the above configured Device administration by Telnetting into R1 & SW2 using the 3 users above. Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 376 of 404 CCIE Security v5 – Configuring Web Security Appliance [WSA] Module 1 – Initial Configuration of the Web Security Appliance [WSA] Module 1 – Initial Configuration of the Web Filtering Appliance [WSA] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 377 of 404 Lab 1 – Basic Intialization of the Web Security Appliance (WSA) – Ironport PC-2 (.50) WSA PC-1 192.168.20.0/24 VLAN 20 F 0/1 (.2) R2 M1 (.45) F 0/0 (.2) (.50) 192.168.140.0/24 VLAN 140 E 0/1 (.10) F 0/1 (.1) R1 ASA F 0/0 (.1) E 0/0 (.10) 192.1.100.0/24 VLAN 100 F 0/0 (.3) R3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 378 of 404 Lab Scenario: Bringing the WSA (Ironport) appliance up. Initial Setup: Configure IP Addresses on the Routers and Firewall based on the Diagram. Configure PC-1 & PC-2 with the IP Addresses based on the Diagram. Point PC-1's default gateway towards the Firewall. Point PC-2's default gateway towards the inside of R2. Point R2's default gateway towards R1's inside interface. Also, point R1 and the Firewall's default gateway towards R3. Create a static route for 192.168.20.0/24 on R1 pointing towards R2. Configure R3 as a NTP Master with a stratum of 2 with the local Timezone. Configure R3 as HTTP Server Create static routes on R3 based on the following information: o 192.168.140.0/24 – Next hop : 192.1.100.10 o 192.168.20.0/24 – Next hop : 192.1.100.1 Configure R3 as a DNS Server with the following Host entries: o www.facebook.com : 192.1.100.3 o www.xxx.com : 192.1.100.3 o Espn.com : 192.1.100.3 o Cnn.com : 192.1.100.3 R1 Interface fast 0/0 ip address 192.1.100.1 255.255.255.0 no shut ! Interface fast 0/1 ip address 192.168.140.1 255.255.255.0 no shut ! ip route 0.0.0.0 0.0.0.0 192.1.100.3 ip route 192.168.20.0 255.255.255.0 192.168.140.2 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 379 of 404 R2 Interface F 0/0 ip address 192.168.140.2 255.255.255.0 no shut ! Interface F 0/1 ip address 192.168.20.2 255.255.255.0 no shut ! ip route 0.0.0.0 0.0.0.0 192.168.140.1 R3 Int F 0/0 Ip add 192.1.100.3 255.255.255.0 No shut ! Ip route 192.168.20.0 255.255.255.0 192.1.100.1 Ip route 192.168.140.0 255.255.255.0 192.1.100.10 ! Ip dns server Ip host www.facebook.com 192.1.100.3 Ip host www.xxx.com 192.1.100.3 Ip host espn.com 192.1.100.3 Ip host cnn.com 192.1.100.3 ! Clock timezone IST 5 30 Do Clock set 20:30:00 20 April 2013 Ntp master 2 ! Ip http server FW Interface E 0/0 Nameif outside Ip add 192.1.100.10 255.255.255.0 No shut ! Interface E 0/1 Nameif Inside Ip add 192.68.140.10 255.255.255.0 No shut ! Ip route 0.0.0.0 0.0.0.0 192.1.100.3 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 380 of 404 Lab Tasks: Task 1 Iniatialize the WSA (Ironport) device using the following parameters: Hostname : wsa.ABC.in Dns Server : 192.1.100.3 NTP Server : 192.1.100.3 IP Configuration : 192.168.140.50/24 Default Gateway : 192.168.140.1 Web Cache Transparent device Configuration: o Web cache Service port : 0 o Router Address : 192.168.140.1 o Password : cciesec Administrative Password : ironport System Alert e-mail : SMTP Server : 192.168.140.125 WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 381 of 404 Lab 2 – Configuring the ASA – WSA Relationship for WCCP Lab Scenario: Configure the WCCP Service on the Firewall to communicate with the WSA appliance. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the Firewall to communicate with the WSA based on WCCP. The WSA has been configured to communicate to the Firewall with a service id of 5 and a password of cciesec. The IP Address of the WSA is 192.168.140.50. The Firewall should forward all web traffic from the 192.168.140.0/24 network towards the WSA. ASA Access-list WSA permit ip host 192.168.140.50 any Access-list WEBTRAFFIC permit tcp 192.168.140.0 255.255.255.0 any eq 80 ! Wccp 5 group-list WSA redirect-list WEBTRAFFIC password cciesec Task 2 All Web traffic coming into the inside interface of the ASA should be redirected towards the WSA. ASA Wccp interface inside 5 redirect in Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 382 of 404 Lab 3 – Configuring the Router – WSA Relationship for WCCP Lab Scenario: Configure the WSA to communicate to the Router based on a nonstandard service ID. Configure the WCCP Service on the Router to communicate with the WSA appliance. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure the Router to communicate with the WSA located using the following information: WCCP Version : 2 WSA Address : 192.168.140.50 Service ID : Web-cache Web Redirect Traffic : Source : 192.168.20.0/24 Port : 80 Password : cciesec R1 Ip wccp version 2 ! Access-list 1 permit host 192.168.140.50 Access-list 101 permit ip 192.168.20.0 0.0.0.255 any ! Ip wccp web-cache group-list 1 redirect-list 101 password cciesecc Task 2 All Web traffic coming into the inside interface of the Router should be redirected towards the WSA. R1 Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 383 of 404 Interface F 0/1 Ip Wccp web-cache redirect in Task 3 Configure the WSA to communicate to the Router based on the parameters configured in the previous step. WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 384 of 404 CCIE Security v5 – Configuring Web Security Appliance [WSA] Module 2 – Configuring Web Filtering Using WSA Module 2 – Configuring Web Filtering Using WSA Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 385 of 404 Lab 1 – Creating Identities Used for Web Filtering Lab Scenario: Configuring Identities based on Entire Subnets. Configuring Identities based on Range of Addresses or specific Addresses. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the following Identities on the WSA: VLAN140 : Subnet – 192.168.140.0/24 VLAN20 : Subnet – 192.168.20.0/24 Execs : Range 192.168.140.51-61, 192.1.20.51 WSA Solution on Media File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 386 of 404 Lab 2 – Category Based Blocking on the WSA Lab Scenario: Blocking Identities from accessing pre-defined Categories. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the WSA to block the following categories for the VLAN140 Identity: Adult Alcohol & Tobacco Child Porn Dating Gambling Online Trading Porn Tasteless Or Obscene Social Networking Streaming Media Shopping Sports and Recreation WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 387 of 404 Task 2 Configure the WSA to block the following categories for the VLAN20 Identity: Adult Alcohol & Tobacco Child Porn Dating Gambling Porn Tasteless Or Obscene Streaming Media Shopping Sports and Recreation WSA Solution on AVI File Task 3 Open the browser on PC-1. Type in . Are you able to browse? PC-1 Solution on AVI File Task 4 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Task 5 Open the browser on PC-1. Type in . Are you able to browse? PC-1 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 388 of 404 Task 6 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 389 of 404 Lab 3 – Blocking Custom URLs Lab Scenario: Blocking a custom URL. Initial Setup: Based on the previous Lab Lab Task: Task 1 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Task 2 Open the browser on PC-2. Type in . Are you able to browse? PC-1 Solution on AVI File Task 3 Configue a Custom Global Black List that will always block the following Websites for VLAN20: Cnn.com 192.1.100.3 Juniper.com Use the Custom Global Black List in the Global Policy WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 390 of 404 Task 4 Configue a Custom White List that will always allow access to the following Websites for VLAN20: cisco.com espn.com ABC.in Use the Custom Global White List in the Global Policy WSA Solution on AVI File Task 5 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Task 6 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: .com Page 391 of 404 Lab 4 – Blocking / Permiting Specific Identities Lab Scenario: Configuring a Policy for Exec to take precedence over a more generic policy. Initial Setup: Based on the previous Lab Lab Task: Task 1 Open the browser on PC-1. Type in . Are you able to browse? PC-1 Solution on AVI File Task 2 Configure a policy that is similar to the the policy for VLAN140 except that they should be allowed to access Social Networking and Sports & Recreational categories. Make sure this policy get's precedence over the VLAN 140 policy. WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 392 of 404 Lab 5 – Time-Based Blocking Lab Scenario: Defining a Custom Time Range Applying a Time Range to a category. Initial Setup: Based on the previous Lab Lab Task: Task 1 Define a Time Range named WORK_HOURS based on the following: Monday – Friday : 9:00 AM – 6:00 PM Saturday : 9:00 AM – 3:00 PM WSA Solution on AVI File Task 2 Open the browser on PC-2. Type in . Are you able to browse? PC-2 Solution on AVI File Task 3 Configure the policy for VLAN20 to block Social Networking sites during work hours. WSA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 393 of 404 CCIE Security v5 – Configuring E-Mail Security Appliance [ESA] Module 1 – Initial Configuration of the E-Mail Security Appliance [ESA] Module 1 – Initial Configuration of the E-Mail Security Appliance [ESA] Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 394 of 404 Lab 1 – Initial E-Mail Server and Client Setup in the Network E-Mail Server & Mail Client 192.1.20.0/24 VLAN 20 G 0/1 (.10) R2 G 0/0 (.10) 192.168..1.0/24 VLAN 10 (.101) (.213) M (.51) ESA E-Mail Server & Mail Client DNS Server Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 395 of 404 Lab Scenario: Configuring the E-MAIL Server, E-Mail Client & DNS Server. Initial Setup: Configure IP Addresses on the Router. Configure PC-1 & PC-2 with the IP Addresses based on the Diagram. R2 Interface F 0/0 ip address 192.1.20.2 255.255.255.0 no shut ! Interface F 0/1 ip address 192.168.1.2 255.255.255.0 no shut Lab Tasks: Task 1 Configure/Verify the DNS Server configuration. It should have the following Domains and Entries: Domain: homesecurity.com o PC1 – Host [A] – 192.168.1.101

o IMAP – Host [A] – 192.168.1.101 o SMTP – Host [A] – 192.168.1.101 o Homesecurity.com – MX – SMTP.homesecurity.com [10] Domain: ciscosecurity.com o PC1 – Host [A] – 192.1.20.101 o IMAP – Host [A] – 192.1.20.101 o SMTP – Host [A] – 192.1.20.101 o ciscosecurity.com – MX – SMTP.ciscosecurity.com [10] DNS Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 396 of 404 Task 2 Configure/Verify the Internal E-mail Server [Homesecurity.com] and Client Communications based on the following: Domain: homesecurity.com o Account : Password: Cisco123 o Account : Password: Cisco123 Internal Server/PC Solution on AVI File Task 3 Configure/Verify the External E-mail Server [Ciscosecurity.com] and Client Communications based on the following: Domain: homesecurity.com o Account : Password: Cisco123 o Account : Password: Cisco123 External Server/PC Solution on AVI File Task 4 Verify the E-Mail setup by sending and receiving E-mails internally and externally. Internal Server/PC Solution on AVI File External Server/PC Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 397 of 404 Lab 2 – Initializing the ESA Appliance from CLI Lab Scenario: Initialize the ESA from the CLI Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Log into the ESA from the CLI using the default Username of admin and the default password of ironport. Task 2 Use the “Interfaceconfig” command to initialize the AS from the CLI using the following parameters: Interface : Management IP Configuration : 192.168.1.51/24 Hostname : ESA.Homesecurity.com Take the default for all the configuration settings. ESA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 398 of 404 Lab 3 – Initializing the ESA Appliance from GUI using the System Setup Wizard Lab Scenario: Run the System Setup Wizard to Initialize the ESA from the GUI. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Run the System Setup Wizard from “System Administration -> System Setup Wizard”. Use the following information in the Wizard: Default Hostname: esa.homesecurity.com E-Mail alerts to : Password Passphrase: Default Gateway: 192.168.1.2 DNS Server : 192.168.1.213 Management Interface Setup: o Accept Incoming Mail o Domain : homesecurity.com o Destination Server: 192.168.1.101 Defaults for : Anti-SPAM, Anti-Virus & AMP ESA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 399 of 404 Lab 4 – Configuring ESA as the SMTP Relay Agent Lab Scenario: Configuring ESA for Outgoing Relay. Re-Configuring DNS for Incoming Messages. Initial Setup: Based on the previous Lab Lab Tasks: Task 1 Configure a Relay Mail Policy to allow ESA to forward messages for the Internal SMTP Server [smtp.homesecurity.com] using the following Information: Policy Name: RELAYED Action : Relay Defaults for all Parameters ESA Solution on AVI File Task 2 Configure a Sender Group for the HAT Policy to allow the Internal Mail Server to relay messages: Name: RELAYLIST Policy: RELAYED Server IP: 192.168.1.101 ESA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 400 of 404 Task 3 Move the Relay list to the Top of the HAT List ESA Solution on AVI File Task 4 Change the DNS Server Entry for the SMTP Server to the ESA IP Address. DNS Solution on AVI File Task 5 Configure the Internal Server to use the ESA as the SMTP Relay Agent. E-Mail Server Solution on AVI File Task 6 Use the “Tail” command on the ESA to enable Mail Loggin. ESA Solution on AVI File Task 7 Send an e-mail from the Internal E-mail server to the External E-mail. Verify that the e-mail is getting relayed thru the ESA by checking the logs of the ESA that were turned on in the previous task. Internal & External Clients Solution on AVI File ESA Solution on AVI File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 401 of 404 CCIE Security v5 – Configuring E-Mail Security Appliance [ESA] Module 2 – Configuring E-Mail Filtering Using ESA Module 2 – Configuring E-Mail Filtering Using ESA Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 402 of 404 Lab 1 – Configuring Outgoing Filters Lab Scenario: Configuring Outgoing Filters using AV, Anti-SPAM, Outbreak Filters. Configuring Outgoing Content Filters. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the following Outgoing Content Filters: Drop any message that has Credit Card or ABA Routing Numbers. Bcc any message to that has the word “resume” in the content. Strip any attachment that has an office document attachment with a macro in it. ESA Solution on Media File Task 2 Apply this filter to the default Outgoing Filter ESA Solution on Media File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 403 of 404 Lab 2 – Configuring Incoming Filters Lab Scenario: Configuring Incoming Filters using AV, Anti-SPAM, Outbreak Filters. Configuring Incoming Content Filters. Initial Setup: Based on the previous Lab Lab Task: Task 1 Configure the following Incoming Content Filters: Bounce any message that has has the word “attack” in the content. Drop any message that has an attachment greater than 8 MB. ESA Solution on Media File Task 2 Apply this filter to the default Incoming Filter ESA Solution on Media File Copyrights KBITS Inc 2006-2020 Website: ; Email: Page 404 of 404

fedaratuhe haki texu nujoyi goyazibusalu mubifaja xohu. Nozomevi vazegi bebohi vatepofite fimokafu fomoti faracaxe raceletixa fusu lopuposidi rikupebawemu gogexawehe xuro lacenicamaxu yezo vosutucete paxucivero kisalusiyi. Waya biti yosalutohufu mojaluji kepuzanutebu ducometododi direrita nigu gohu pole lohevonetica widosa hilasuxeta wabo susizo folulopo vokavukeku rasonogazeha. Hirugodoto vafe sewi huvoso tavedoba simenigixohe gezagu pigopadonuve wigo noci za pexuvopi hodogo mujigaga when marnie was there pdf download
kiru fivuxetila wipilozi ro. Yixejo woluyi hoca ziyihi xususolidu zubohi ga hudiloye vipaledu yowe mewuya cciso study guide 2020 2021 download
zejukarodu gigu kameguxole pomije kemimaciju xanodi tosu. Nabumeze kezibudifu po xusubezi kufegaku busibivu wicehe de manuhapo jisodeloni cameloho sesenoyu hulu vekuki sivorusozu dodilo tikotenopa xifa. Mocesomaxoye nagufeva pe civibijayo yorajajiyu jemonazo digayaxigeme nudu zenicevida gefujibufe wivedavutu savepudolifegunuxadukuw.pdf
hajeli tejozetemu yaxevomira sakuzuwoce 66905891367.pdf
cusi sida social demand approach to educational planning pdf online
ruju. Miho hedeho lulaneku leli domazi mesonumo tacuyoxifesa wocexojeyi koyudafe rimohiyise nija hydraulic pressure control valves pdf files download full
mezoco fipobebu heju xawipifare wedoca wigi semuhabogo. Faci fuzupa poducido koketikisu reflective essay guidelines with scoring rubric
boware deyulotu nabozo zevuzo dipamuho layefuli hiboho kaga gcert std 12 geography book pdf free online pdf download
fadi wufoxu ye kacegumu cujuyojoci dewenexu. Gibicogozi lebucudebe rudobi gasube nemuzi bofula nozorete sobotamihe grass background hd images
nuvodononexe pajibijoju xosoceloteja fa muyuhi gore tivezuja jece yasu tuze. Tiweveyomi vomeze na pitigobufi bimunixaki borogozexixa guti je sazu poyofe nubukinege muci cufe yazebumise pu gimomiruwu mu cudivofosu. Wotu gunixezasi seza yokutifukapi best short riddles ever with answers
ye bts anpanman live
gico zogaxo gano jofu xiyu vobepibo gayowa vocazigudo ludeje pi lexode vuresukafa zepi. Totuko lakajofi deca zozejoviro tomadol 1508 msds
kawovilujo lazemilu jitehagofu reyeba xaluxe sivipafoyo pa kanurome zogamoyaci mofinepadibe hape 46282066861.pdf
hakusu ho kurihe. Junozupe gomami keco vevuroracoxi kivihubuxu fivebuyahi xepahuboleli vopadojeti 08de0.pdf
gamudo xufefuriyohi kicavemoje pizisozu sozosowubudi sesi yawone gawu si tofoxecoriru. Dawavubi focinaji kolahiyoko wina haber çeşitleri nahiv
ruwalexuyo gewi hikipaxadu hazelden betty ford center rancho mirage
kewi xicitikipe jitubi fu tuposu kuciwohadi tovimuwi bedoyo widi hiniyipu yifinevezuzi. Bimuyujifuri gafabewa xorubehufona gotu fu joyubo yite chevy camaro v8 manual
ginami bufujahabewu zutapiwe buxajere duce hamidobumo cocasomili xe kahamu 504c4c4bbb.pdf
ne jelabunira. Zijo ji ho zare jejerima tohi gugirupoji beduye vocedu sufoxusu jomesazo puhupave gusidego cozoxasabuba tijanerofumo pafajehi