RAAUZYUW RUEOMFB1441 2681724-UUUU--RUCBACM.
ZNR UUUUU ZUI RUEOMCF0908 2681724
R 251706Z SEP 02 PSN 902154L21
FM JOINT STAFF WASHINGTON DC//JSJ6//
TO RUEKJCS/JOINT STAFF WASHINGTON DC
RUEKJCS/CJCS WASHINGTON DC
RUEADWD/CSA WASHINGTON DC
RUENAAA/CNO WASHINGTON DC
RUEAHQA/CSAF WASHINGTON DC
RUEACMC/CMC WASHINGTON DC
RUCAACC/USCINCCENT MACDILL AFB FL
RUCBACM/USCINCJFCOM NORFOLK VA
RUCQSOC/USCINCSOC MACDILL AFB FL
RUMIAAA/USCINCSO J6 MIAMI FL
RUMIAAA/USCINCSO MIAMI FL
RUPESPA/USCINCSPACE PETERSON AFB CO
RUCUSTR/USCINCSTRAT OFFUTT AFB NE
RUEJDCA/DISA ACP-AIG WASHINGTON DC
RUETIAA/DIRNSA FT GEORGE G MEADE MD
ZEN/USCINCEUR VAIHINGEN GE
ZEN/USCINCPAC HONOLULU HI
INFO RUEKJCS/SECDEF WASHINGTON DC//

PAGE 02 RUEOMFB1441 UNCLAS
BT
UNCLAS
SECTION 1 OF 3
QQQQ
SUBJ: FIREWALL GUIDANCE
UNCLAS
MSGID/GENADMIN/J6K//
SUBJ/FIREWALL GUIDANCE//
REF/A/DOC/NSTISSP NO. 11/JAN 2000//
REF/B/MEMO/OASD (C3I)/NATIONAL INFORMATION ASSURANCE
ACQUISITION
POLICY/06 AUG 02//
POC/RON STEPHENS/LTC/JS J6K/LOC:PENTAGON/TEL:703-614 5985
/EMAIL:RON.STEPHENS@JS.PENTAGON.MIL//
RMKS/1. INTRODUCTION: THIS MESSAGE PROVIDES A SET OF
COORDINATED
MINIMUM FIREWALL ARCHITECTURAL AND CONFIGURATION "BEST
PRACTICES" AS
GUIDANCE FOR USE ON THE NIPRNET BY COMBATANT COMMANDS,
MILITARY

SERVICES, AND DOD AGENCIES (C/S/As) IN SUPPORT OF THE
DEFENSE-IN-DEPTH STRATEGY. THE GUIDANCE ENCOMPASSES THE
FIREWALL
ARCHITECTURE DEPLOYMENT STRATEGY DETAILED IN DEFENSE-IN-
DEPTH:

PAGE 03 RUEOMFB1441 UNCLAS
INFORMATION ASSURANCE (IA) AND COMPUTER NETWORK DEFENSE,
CJCSM
6510.01
(DRAFT), WHICH IS CURRENTLY IN COORDINATION. THIS MESSAGE
PROVIDES
INTERIM GUIDANCE FOR FIREWALL IMPLEMENTATION AND
CONFIGURATION FOR
C/S/As UNTIL CJCSM 6510.01 IS SIGNED. REFERENCES TO DRAFT
DOCUMENTS
ARE
FOR INFORMATION ONLY.
2. BACKGROUND: C/S/As ARE RESPONSIBLE FOR DEPLOYING AND
CONFIGURING
FIREWALLS AND OTHER SUPPLEMENTAL DEFENSE-IN-DEPTH
TECHNOLOGIES TO
PROTECT THEIR NETWORKS. UNDER THIS OPERATIONAL ENVIRONMENT,
C/S/As
HAVE DEVELOPED THEIR OWN UNIQUE FIREWALL CONFIGURATION
POLICIES.
INTERCONNECTED DOD NETWORKS, HOWEVER, OPERATE IN A SHARED-
RISK
ENVIRONMENT AND NEED TO MEET MINIMUM CONFIGURATION
STANDARDS.
WITHOUT AN ESTABLISHED FIREWALL CONFIGURATION BASELINE, DOD
FIREWALL
CONFIGURATIONS DIFFER AMONG THE VARIOUS ORGANIZATIONS. THE
DRAFT
NIPRNET PORTS AND PROTOCOLS POLICY, FEBRUARY 2002, PROVIDES
CONFIGURATION SETTINGS AND COUNTERMEASURES FOR MILITARY
SERVICES
AND DOD AGENCIES TO MEET THE DEMANDS OF THIS SHARED RISK
ENVIRONMENT.
THE POINT OF CONTACT FOR THE PORTS AND PROTOCOLS POLICY IS THE
DEFENSE

INFORMATION SYSTEMS AGENCY (DISA) CENTER FOR INFORMATION ASSURANCE ENGINEERING (CIAE), PHONE: (703) 882-0448.

3. CONCEPT: THIS FIREWALL CONFIGURATION GUIDANCE IS BASED ON THE FIREWALL PHILOSOPHY OF "DENY-BY-DEFAULT" WHICH MANDATES THAT ALL PORTS, PROTOCOLS AND SERVICES BE BLOCKED OR DENIED FOR INBOUND AND OUTBOUND TRAFFIC UNLESS SPECIFICALLY REQUIRED AND APPROVED FOR OPERATIONAL USE. GIVEN THE INCREASINGLY LARGE NUMBER OF HIGHLY VULNERABLE SERVICES AND PROTOCOLS, CAREFUL CONSIDERATION SHOULD BE GIVEN PRIOR TO ENABLING ANY SERVICE OR PROTOCOL THROUGH THE FIREWALL.

4. SECURITY POLICY: ONE OF THE PRIMARY FUNCTIONS OF A FIREWALL IS TO SUPPORT AND IMPLEMENT AN ORGANIZATION'S SECURITY POLICY. EACH C/S/A SHOULD SUPPORT THE DEVELOPMENT OF A COMMON DOD BASELINE PORTS AND PROTOCOLS SECURITY POLICY (PPSP) TO ENSURE THAT COMMON DOD SECURITY AND INTEROPERABILITY REQUIREMENTS AS WELL AS INDIVIDUAL C/S/A NEEDS ARE MET. THE C/S/A SHOULD DEVELOP AN INTERNAL SECURITY POLICY THAT IS AT LEAST AS RESTRICTIVE AS THE COMMON DOD PPSP. THE FIREWALL-RELATED

SECURITY POLICY, AS A MINIMUM, IDENTIFIES THE FOLLOWING: ALL NETWORK ASSETS PROTECTED BY THE FIREWALL, ALL NETWORK SERVICES REQUIRED TO SUPPORT SYSTEMS PROTECTED BY THE FIREWALL, ALL NETWORK SERVICES REQUIRED TO SUPPORT SYSTEMS AND THE SYSTEM'S CRITICALITY, THREATS, MITIGATION

MEASURES, REQUIRED AUDIT ITEMS, INCIDENT RESPONSE PROCEDURES,
AND
RESPONSIBILITIES/TRAINING REQUIREMENTS FOR ALL CLEARED USERS,
ADMINISTRATORS AND MANAGERS.
5. IMPLEMENTATION: FIREWALL IMPLEMENTATION SHOULD INCLUDE:
A. COORDINATION WITH THE SUPPORTING MILITARY SERVICE'S
NETWORK
OPERATIONS CENTER (NOC) AND COMPUTER EMERGENCY RESPONSE
TEAM (CERT)
AS WELL AS DOD NOCS AND CERT.
B. AFTER THE C/S/A UTILIZES ITS OWN PRIORITIZATION AND PROCEDURES
FOR NETWORK RESTORATION AND INVESTIGATION, THE SUPPORTING NOC
AND
CERT
SHOULD COORDINATE ACCESS TO THE C/S/A's INTERNAL NETWORK TO
SUPPORT
INCIDENT INVESTIGATION OR NETWORK RESTORATION. ACCESS SHOULD
BE
PROVIDED THROUGH PHYSICAL CONNECTIONS TO THE INTERNAL
NETWORK
OR THROUGH PROPERLY ENCRYPTED (BASED ON THE SENSITIVITY OF
DATA)
CONNECTIONS OVER A WIDE AREA NETWORK (WAN). ALL IA PRODUCTS

(INCLUDING FIREWALLS) PURCHASED AFTER 1 JULY 2002 MUST BE
EVALUATED IN ACCORDANCE WITH NSTISSP NO. 11, REF A, AND THE
NATIONAL
INFORMATION ASSURANCE ACQUISITION POLICY MEMORANDUM, REF B.
THE
EVALUATED ASSURANCE LEVEL (EAL) MUST MAP TO THE LEVEL OF
ROBUSTNESS
REQUIRED FOR THE LEVEL OF DATA.
6. ARCHITECTURE: WHILE FIREWALLS AT ALL NETWORK BOUNDARIES
REPRESENT THE CRITICAL COMPONENT OF A STRONG NETWORK
DEFENSE, A WELL
DEVELOPED NETWORK ARCHITECTURE INCORPORATING SEVERAL OTHER
KEY IA
COMPONENTS IS EQUALLY IMPORTANT. THE C/S/A SHOULD ENSURE THEIR
GLOBAL, REGIONAL, AND POST/BASE/CAMP/STATION ARCHITECTURES
AND
COMPONENTS COMPLY WITH THESE GUIDELINES. THESE COMPONENTS
INCLUDE:

A. A BORDER ROUTER THAT SHOULD BE CONFIGURED BETWEEN THE FIREWALL AND THE EXTERNAL NETWORK. THIS ROUTER SHOULD HAVE AN ACCESS CONTROL LIST AND COMPLEMENT THE FIREWALL CONFIGURATION. ALL UNNECESSARY SERVICES (I.E. TCP/UDP SMALL SERVERS, DIRECTED BROADCASTS, PROXY ARP, ETC.) AND SOURCE ROUTING SHOULD BE DISABLED ON THIS ROUTER.

B. A DEMILITARIZED ZONE (DMZ) SHOULD BE IMPLEMENTED. A DMZ IS A DEDICATED NETWORK SEGMENT THAT PROVIDES NETWORK CONNECTIVITY FOR AN ORGANIZATION'S PUBLICLY ACCESSIBLE SERVERS (I.E. EXTERNAL DNS, WEB, FTP). THE DMZ SHOULD BE LOCATED ON THE NETWORK SEGMENT CONNECTING THE FIREWALL TO THE BORDER ROUTER OR ON A DEDICATED NETWORK SEGMENT CONNECTED TO THE FIREWALL (IN THIS CASE, THE FIREWALL WOULD REQUIRE A MINIMUM OF THREE INTERFACES). ACCESS CONTROL LISTS SHOULD BE CONFIGURED ON THE FIREWALL AND BORDER ROUTER TO RESTRICT EXTERNAL ACCESS TO ONLY THE SERVERS ON THE DMZ ACCORDING TO THE C/S/A NETWORK SECURITY POLICY, WITH FEW DOCUMENTED EXCEPTIONS.

C. AN INTRUSION DETECTION SYSTEMS (IDS) SHOULD BE USED IN CONJUNCTION WITH A FIREWALL. PLACEMENT OF THE IDS SHOULD BE IN ACCORDANCE WITH THE C/S/A SECURITY POLICY.

D. AN APPLICATION LEVEL (ALSO SOMETIMES CALLED AN APPLICATION PROXY OR PROXY) TYPE OF FIREWALL IS RECOMMENDED TO ENFORCE WEB USAGE POLICIES, CONSERVE BANDWIDTH, AND/OR TO IMPROVE PERFORMANCE FOR FREQUENTLY ACCESSED SITES.

E. THE FIREWALL SHOULD BE HOSTED ON A DEDICATED HARDWARE PLATFORM.

7. FIREWALL SECURITY REQUIREMENTS: IT IS RECOMMENDED THAT ALL C/S/As MEET THE FOLLOWING FIREWALL SECURITY REQUIREMENTS:

SECTION 2 OF 3

QQQQ

A. THE FIREWALL SHOULD BE LOCATED IN A PHYSICALLY SECURE LOCATION.

B. FOR ALL SOFTWARE BASED FIREWALLS, UNDERLYING OPERATING SYSTEMS (OS) SHOULD BE HARDENED IN ACCORDANCE WITH THE MOST RECENT NSA AND DISA POLICIES PERTAINING TO THE PARTICULAR OS PRIOR TO LOADING THE FIREWALL. FOR EXAMPLE, REFER TO "GUIDE TO SECURING MICROSOFT WINDOWS NT NETWORKS", FEBRUARY 3, 2000, VERSION 4.0 PREPARED BY THE NETWORK ATTACK TECHNIQUES DIVISION OF THE SYSTEMS AND NETWORK ATTACK CENTER (SNAC). TO OBTAIN A CD, CALL THE NATIONAL SECURITY AGENCY (NSA) IA SERVICE CENTER AT 1-800-688-6 115.

C. THE FIREWALL AND ANY CORRESPONDING OS SHOULD BE KEPT UP TO DATE WITH THE MOST CURRENT PATCHES AND BUG FIXES AND HAVE CURRENT MAINTENANCE FOR BOTH THE HARDWARE AND SOFTWARE. PATCHES AND BUG FIXES SHOULD BE OBTAINED THROUGH DOD CHANNELS, IF AVAILABLE, AND IN COORDINATION WITH CONFIGURATION CONTROL. INSTALLATION OF PATCHES AND BUG FIXES SHOULD BE COMPLIANT WITH IAVAS AND SERVICE EQUIVALENT DIRECTIVES.

D. THE FIREWALL SHOULD EMPLOY NETWORK ADDRESS TRANSLATION (NAT) TO HIDE INTERNAL IP ADDRESSES TO THE MAXIMUM EXTENT POSSIBLE. CONFIGURE NAT FIREWALLS SO THAT OUTBOUND NETWORK TRAFFIC APPEARS AS IF THE TRAFFIC HAD ORIGINATED AT THE FIREWALL. ANY EXCEPTIONS SHOULD BE APPLIED ON A CASE-BY-CASE BASIS AND BE FULLY DOCUMENTED. NO LOCAL FIREWALL POLICY SHOULD BE IMPLEMENTED WHICH PROHIBITS OR RESTRICTS TRANSLATED ADDRESSES INBOUND WHEN RESTRICTING ACCESS TO

SYSTEMS OR NETWORKS TO SPECIFIC SOURCES ADDRESSES. IF A
SITUATION
REQUIRES AN EXCEPTION TO THIS RECOMMENDATION, IT SHOULD BE
FULLY
DOCUMENTED.
E. ANTI-SPOOFING (INGRESS AND EGRESS FILTERING): ALL TRAFFIC ON
THE
FIREWALL'S EXTERNAL INTERFACE THAT APPEARS TO BE COMING FROM
INTERNAL NETWORK ADDRESSES SHOULD BE REJECTED.
F. ALL FACTORY DEFAULT ACCOUNT NAMES AND PASSWORDS MUST BE
CHANGED.
ALL ACCOUNTS THAT ARE NOT REQUIRED SHOULD BE REMOVED.
DEFAULT SECURE
SOCKET LAYER CERTIFICATES FOR APPLICATIONS SUCH AS SSH OR
SECURE
REMOTE ADMINISTRATION SHOULD LIKEWISE BE CHANGED, INCLUDING
SNMP
READ/WRITE COMMUNITY STRINGS.
G. DISABLE ANY CAPABILITY OR FEATURE NOT REQUIRED FOR FIREWALL

OPERATION. THIS SHOULD ELIMINATE EXPOSURE TO POSSIBLE SECURITY
VULNERABILITIES.
H. THE FIREWALL SHOULD REBOOT TO A KNOWN CONFIGURATION TO
PREVENT
ATTACKS WHICH INVOLVE CONFIGURATION CHANGE AND REBOOT.
I. STORE SYSTEM CONFIGURATION INFORMATION ON READ-ONLY MEDIA
OR ON
OFF-LINE STORAGE. STORE BACK-UP MEDIA AT AN OFF-SITE STORAGE
LOCATION.
J. FIREWALL CONTENTS: THE FIREWALL SHALL ONLY CONTAIN
SOFTWARE OR
FILES DIRECTLY RELATED TO THE FUNCTIONING OF THE FIREWALL.
REMOVE
UNAUTHORIZED COMPILERS, EDITORS, AND OTHER PROGRAM
DEVELOPMENT TOOLS
FROM OPERATIONAL FIREWALL SYSTEMS, WHICH COULD BE USED TO
INSTALL OR
EXECUTE HOSTILE CODE SUCH AS TROJAN HORSES OR BACKDOORS.
K. FIREWALL ADMINISTRATION: THE NUMBER OF FIREWALL ACCOUNTS
SHOULD BE
LIMITED TO ONLY THOSE ABSOLUTELY NECESSARY. CHANGES, WHICH
AFFECT

ACCESS CONTROL LISTS, SERVICES, FILTERS, OR PROXIES FIRST SHOULD
BE
COORDINATED WITH AND APPROVED BY THE POLICY-MAKING
AUTHORITY FOR
THAT FIREWALL.
L. FIREWALL AUTHENTICATION REQUIREMENTS: UPON AVAILABILITY OF
CAPABILITY, THE FIREWALL SHALL UNIQUELY IDENTIFY AND
AUTHENTICATE
THE CLAIMED IDENTITY OF ANY USER BEFORE GRANTING ACCESS TO THE

PAGE 05 RUEOMFB1442 UNCLAS
FIREWALL'S ADMINISTRATION INTERFACE. AN AUTHENTICATION
METHOD IS
RECOMMENDED FOR ALL FIREWALL MANAGEMENT. DEVELOP
MIGRATION PLANS TO
BRING ALL FIREWALLS INTO COMPLIANCE WITHIN 12 MONTHS AFTER
TECHNOLOGY AVAILABILITY. ALTHOUGH REMOTE MANAGEMENT IS
DISCOURAGED,
IF REQUIRED, REMOTE MANAGEMENT SESSIONS SHOULD BE CONDUCTED
THROUGH A
SECURE TRANSPORT (I.E. HTTPS, SSL, VPN, IPSEC) FROM TRUSTED
MANAGEMENT TERMINALS WITHIN A PROTECTED NETWORK, INCLUDING
REMOTE
PROTECTED NETWORKS.
M. AUDIT REQUIREMENTS: AUDITING SHOULD BE IMPLEMENTED AS
PROVIDED BY
THE FIREWALL SOFTWARE WITH THE FOLLOWING MINIMUM
REQUIREMENTS. THE
FIREWALL SHOULD PROVIDE A MEANS TO RECORD A READABLE AUDIT
TRAIL OF
SECURITY-RELEVANT EVENTS AND A MEANS TO SEARCH AND SORT THE
AUDIT
DATA BASED ON SPECIFIC ATTRIBUTES. MINIMUM RECORDED SECURITY
RELEVANT EVENTS SHOULD INCLUDE ALL ACTIVITIES OF
ADMINISTRATORS, ALL
SUCCESSFUL/UNSUCCESSFUL AUTHENTICATION ATTEMPTS, ANY
ACTIVITY CAUGHT
BY THE DENY ALL RULE AT THE END OF THE FIREWALL RULEBASE. AUDIT
LOGS
SHOULD BE REVIEWED DAILY. THE FIREWALL SHOULD PROVIDE A
MEANS TO
IMMEDIATELY NOTIFY THE ADMINISTRATOR OF ANY HIGH PRIORITY
SECURITY-RELEVANT EVENTS (SUCH AS EXCESSIVE FAILED LOGIN
ATTEMPTS)

OR CRITICAL OPERATIONAL EVENTS (SUCH AS NEAR FULL AUDIT LOGS). THE

PAGE 06 RUEOMFB1442 UNCLAS

FIREWALL SHOULD PROVIDE A MEANS TO STORE AUDIT RECORDS TO A DEDICATED SERVER ON THE INTERNAL NETWORK. ACCESS TO THE AUDIT SERVER SHOULD BE LIMITED TO AUTHORIZED PERSONNEL ONLY. AUDIT RECORDS SHOULD BE MAINTAINED FOR A MINIMUM OF SIX (6) MONTHS. WHEN NECESSARY, AUDIT LOGS SHOULD BE WRITTEN TO "WRITE-ONCE" MEDIA.

8. CONFIGURATION MANAGEMENT/MAINTENANCE/TESTING OF THE FIREWALL:

THE FIREWALL SHOULD BE TESTED AND SHOWN TO BE RESISTANT TO ATTACK.

A. THE BASELINE CONFIGURATION OF THE FIREWALL SHOULD BE MAPPED AGAINST THE APPROVED SECURITY POLICY.

B. PERFORM INSTALLATION VERIFICATION TESTING TO VALIDATE THAT COMPONENTS WERE PROPERLY ENTERED WHEN THE FIREWALL WAS INSTALLED.

DOCUMENT THE RESULTS AND KEEP ON FILE FOR REFERENCE.

C. A VULNERABILITY SCANNER SHOULD BE RUN AGAINST THE FIREWALL AND ANY REPORTED VULNERABILITIES CORRECTED PRIOR TO CONNECTING THE FIREWALL TO THE "LIVE" NETWORK. ONCE A SATISFACTORY (I.E. CORRECTED VULNERABILITIES WITH ACCEPTABLE RESIDUAL RISKS) SCAN HAS COMPLETED, THE OUTPUT SHOULD BE SECURELY STORED FOR FUTURE REFERENCE/COMPARISON.

D. VULNERABILITY SCANS SHOULD BE CONDUCTED AT LEAST QUARTERLY AS PART OF ROUTINE MAINTENANCE. VULNERABILITY SCANS SHOULD BE CONDUCTED AGAINST HOSTS INTERNAL TO THE FIREWALL, IN ADDITION TO THE FIREWALL

PAGE 07 RUEOMFB1442 UNCLAS

ITSELF, TO CONFIRM AN ADEQUATE SECURITY POLICY IS BEING ENFORCED.

E. REGULAR UPGRADES/UPDATES TO THE VULNERABILITY SCANNER
SHOULD BE
MAINTAINED TO ENSURE THAT CURRENT VULNERABILITIES HAVE BEEN
INCORPORATED.
F. THE HOST NETWORK SYSTEM SECURITY AUTHORIZATION AGREEMENT
(SSAA)
SYSTEM ARCHITECTURE DESCRIPTION SECTION SHOULD BE UPDATED TO
CLEARLY
IDENTIFY THE FIREWALL LOCATION(S), SERVICES, AND EXACT
FUNCTIONS.
IN ADDITION, THE SSAA SHOULD INCLUDE PLANS FOR CERTIFICATION
AND
RECERTIFICATION, AUDITING OF LOGS, AND POLICIES FOR IDENTIFYING
AND
AUTHENTICATING APPROVED FIREWALL ADMINISTRATORS.
G. BECAUSE THE FIREWALL IS A KEY COMPONENT OF A NETWORK
DEFENSE
POSTURE, THERE SHOULD BE AT LEAST ONE (1) CLEARED, QUALIFIED
FIREWALL ADMINISTRATOR ASSIGNED. A FIREWALL ADMINISTRATOR
SHOULD BE
AVAILABLE FOR EMERGENCY CHANGES IN RESPONSE TO COMPUTER
NETWORK
EVENTS/INCIDENTS.
H. FIREWALL UPGRADES/UPDATES SHOULD BE DOCUMENTED AND
COORDINATED
THROUGH THE CONFIGURATION MANAGEMENT PROCESS.
I. AN ANNUAL REVIEW OF ALL FIREWALL RULES SHOULD BE
CONDUCTED.
9. ADDITIONAL INFORMATION: BASELINE FIREWALL CONFIGURATION
GUIDANCE
FINAL SECTION OF 3
QQQQ
TO ASSIST IN THE INSTALLATION OF A FIREWALL IN AN UNCLASSIFIED
AND
NETWORK CAN BE FOUND AT WEB SITE:
IATF.NET/PROTECTION_PROFILES/FIREWA
LLS.CFM.
ADDITIONAL INFORMATION IS AVAILABLE AT WEBSITE:
MATTCHE.IIIE.DISA.MIL/IASEINFODESK.HTML. NSA GUIDANCE ON
CONFIGURING ROUTERS CAN BE FOUND AT WEBSITE: NSA.GOV UNDER
"SECURITY RECOMMENDATION GUIDES." IN ADDITION, NSA GUIDANCE
FOR
SECURING MICROSOFT WINDOWS NT NETWORKS & APPLICATIONS CAN BE
OBTAINED BY CALLING 1-800 688 6115. FOR NSA INFORMATION ON
SECURING
UNIX NETWORKS, CONTACT 410-854 6529. DISA'S SECURITY TECHNICAL

IMPLEMENTATION GUIDES (STIGS) ON SECURING ENCLAVES, NETWORKS, AND
OPERATING SYSTEMS CAN BE FOUND AT WEBSITE: IASE.DISA.MIL AND IASE.DISA.SMIL.MIL . FIREWALLS AND ROUTERS FUNDAMENTALS, AN INTERACTIVE, MULTIMEDIA WEB BASED TRAINING/COMPUTER BASED TRAINING/(WBT/CBT) PRODUCT FOR LEVEL 1 SYSTEMS ADMINISTRATORS

PROVIDES A HIGH-LEVEL OVERVIEW OF SECURITY ISSUES RELATED TO THE
USE OF FIREWALLS AND ROUTERS. FOR ACCESS TO GUIDES OR FOR ADDITIONAL STIG INFORMATION, CONTACT THE FSO SUPPORT DESK, (717) 267-9264.
//

BT
#1441
NNNN