



Global Knowledge®

Expert Reference Series of White Papers

Using Syslog Effectively for Security Troubleshooting

Using Syslog Effectively for Security Troubleshooting

Douglas B. McKillip, P.E., Global Knowledge Instructor, CCSI, CCSP, CCIE #1851

Introduction

This paper examines the numerous ways that syslog messages can be used to enhance the secure deployment of an infrastructure of equipment from Cisco®. Syslog can not only be an essential auditing tool for network and administrative events, but also can be an effective troubleshooting tool. We will examine the utilization of syslog in the following key areas:

- Configuration change auditing
- Troubleshooting VPNs and Downloadable Access Lists
- Secure reporting using Secure Logging with TCP and Transport Layer Service

Configuration Change Auditing

Starting with Cisco IOS 12.3(4)T, an administrator can configure a router with a series of commands such that any subsequent configuration commands entered will be sent to syslog. Having a recorded audit trail of changes made can provide a valuable tool to troubleshoot possible unexpected outcomes. A sample router configuration dialog is shown below:

```
Router# config t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# logging trap notifications
Router(config)# logging 10.10.2.10
Router(config)# archive
Router(config-archive)# log config
Router(config-archive-log-cfg)# logging enable
Router(config-archive-log-cfg)# logging size 1000
Router(config-archive-log-cfg)# hidekeys
Router(config-archive-log-cfg)# notify syslog
```

The purpose of the **hidekeys** command above is NOT to log the entry of passwords. The display below shows a Kiwi® Syslog Service Manager display, which captures some entered configuration commands. Note that these all appear with the **%PARSER-5-CFGLOG** prefix.

Date	Time	Priority	Hostname	Message
12-01-2009	16:41:37	Local7/Notice	10.20.0.2	33: Dec 1 22:41:52.863: %SYS-5-CONFIG_I: Configured from console by console
12-01-2009	16:41:34	Local7/Notice	10.20.0.2	32: Dec 1 22:41:49.685: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:exit
12-01-2009	16:41:32	Local7/Notice	10.20.0.2	31: Dec 1 22:41:48.054: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:description inside interface of Site1 Router
12-01-2009	16:41:13	Local7/Notice	10.20.0.2	30: Dec 1 22:41:27.763: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:interface FastEthernet0/1
12-01-2009	16:40:58	Local7/Notice	10.20.0.2	29: Dec 1 22:41:14.537: %SYS-5-CONFIG_I: Configured from console by console
12-01-2009	16:40:55	Local7/Notice	10.20.0.2	28: Dec 1 22:41:11.585: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:do wr
12-01-2009	16:40:48	Local7/Notice	10.20.0.2	27: Dec 1 22:41:04.429: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:notify syslog
12-01-2009	16:39:38	Local7/Info	10.20.0.2	26: Dec 1 22:39:58.351: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 10.10.2.10 started - CLI initiated
12-01-2009	16:39:37	Local7/Notice	10.20.0.2	25: Dec 1 22:39:57.351: %SYS-5-CONFIG_I: Configured from console by console

Previously, **aaa** commands were needed to audit configuration commands, and they needed a TACACS+ server to receive them. Unfortunately, this functionality has not yet been introduced for the ASA firewall.

Troubleshooting VPNs

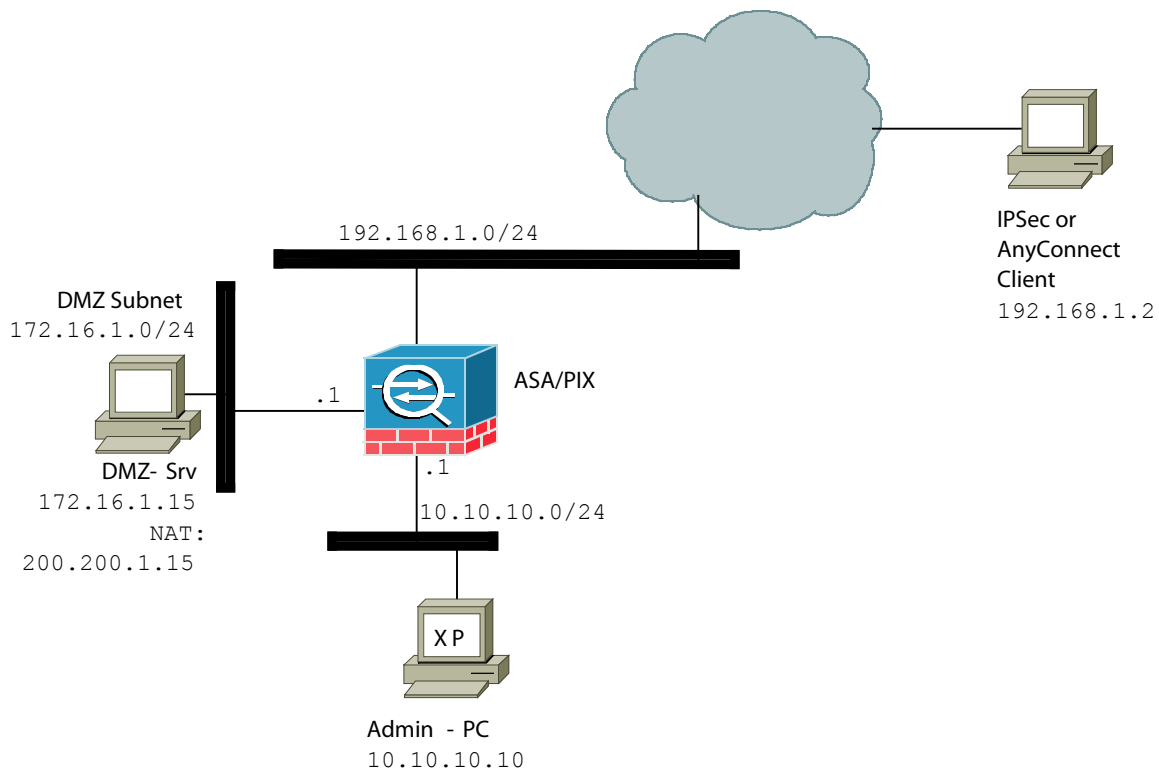
Although the appropriate use of the applicable **debug** command can provide valuable output in troubleshooting VPN connectivity problems, a disadvantage of this approach is that the output cannot be sent to an external server. Instead, administrators either need to spot the key diagnostic message as it quickly scrolls by, or they need to capture the terminal output to disk. By using syslog instead, the information can be kept more easily for later analysis. In addition, syslog servers like the Cisco MARS[®] appliance can be configured with customized rules to generate incidents when raw messages due to VPN misconfiguration occur.

We will examine the following remote access VPN scenarios:

- Wrong IPsec VPN Client Group Name
- Wrong IPsec VPN Client Pre-shared Key
- Missing IPsec VPN Client Address Pool
- Bad User Password and Missing Address Pool for SSL AnyConnect Client

Troubleshooting Scenario

The following scenario will be used to illustrate syslog for use troubleshooting outlined above. A simple simulation of an external client connection to either a PIX (for IPsec) or an ASA (for AnyConnect[®]) was done from a laptop on the same external network as the security appliances, appearing in the traces as **192.168.1.2**. The IPsec Group name is **MYGROUP**. Both the PIX and the ASA in the sections below were booted with OS8.0 code.



Wrong IPSec VPN Client Group Name

A partial output setting the log level to debug appearing on the console is shown below:
(Note that the message which indicates the problem is indicated in bold font.)

logging on

```
pixfirewall(config)# %PIX-5-111008: User 'enable_15' executed the 'log-
ging on' command.
%PIX-7-609001: Built local-host outside:192.168.1.2
%PIX-6-302015: Built inbound UDP connection 5 for out-
side:192.168.1.2/500 (192.168.1.2/500) to identity:192.168.1.202/500
(192.168.1.202/500)
%PIX-7-713236: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR
(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE
(0) total length : 853
%PIX-7-715047: IP = 192.168.1.2, processing SA payload
%PIX-7-715047: IP = 192.168.1.2, processing ke payload
%PIX-7-715047: IP = 192.168.1.2, processing ISA_KE payload
%PIX-7-715047: IP = 192.168.1.2, processing nonce payload
```

```

%PIX-7-715047: IP = 192.168.1.2, processing ID payload
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received xauth V6 VID
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received DPD VID
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received NAT-Traversal ver 02 VID
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received Fragmentation VID
%PIX-7-715064: IP = 192.168.1.2, IKE Peer included IKE fragmentation
capability flags: Main Mode:      True Aggressive Mode: False
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received Cisco Unity client VID
%PIX-4-713255: IP = 192.168.1.2, Received ISAKMP Aggressive Mode
message 1 with unknown tunnel group name 'MYGROUP1'.

```

Wrong IPSec VPN Client Pre-Shared Key

While the above output quickly indicated that the configured group name was wrong, once this error is corrected, spotting a misconfigured pre-shared key requires more lines of output. Notice that the correctly configured group name, **MYGROUP**, appears regularly in the output of the log:

logging on

```

DOUGPIX-515E(config)# %PIX-5-111008: User 'enable_15' executed the
'logging on' command.
DOUGPIX-515E(config)# %PIX-7-713236: IP = 192.168.1.2, IKE_DECODE RE-
CEIVED Message (msgid=0) with payloads : HDR + SA (1) + KE (4) + NONCE
(10) + ID (5) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13)
+ VENDOR (13) + NONE (0) total length : 852
%PIX-7-715047: IP = 192.168.1.2, processing SA payload
%PIX-7-715047: IP = 192.168.1.2, processing ke payload
%PIX-7-715047: IP = 192.168.1.2, processing ISA_KE payload
%PIX-7-715047: IP = 192.168.1.2, processing nonce payload
%PIX-7-715047: IP = 192.168.1.2, processing ID payload
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received xauth V6 VID
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received DPD VID

```

%PIX-7-715047: IP = 192.168.1.2, processing VID payload (output continues, next page)

%PIX-7-715049: IP = 192.168.1.2, Received NAT-Traversal ver 02 VID

%PIX-7-715047: IP = 192.168.1.2, processing VID payload

%PIX-7-715049: IP = 192.168.1.2, Received Fragmentation VID

%PIX-7-715064: IP = 192.168.1.2, IKE Peer included IKE fragmentation capability flags: Main Mode: True Aggressive Mode: False

%PIX-7-715047: IP = 192.168.1.2, processing VID payload

%PIX-7-715049: IP = 192.168.1.2, Received Cisco Unity client VID

%PIX-7-713906: IP = 192.168.1.2, Connection landed on tunnel_group MYGROUP

%PIX-7-715047: Group = MYGROUP, IP = 192.168.1.2, processing IKE SA payload

%PIX-7-715028: Group = MYGROUP, IP = 192.168.1.2, IKE SA Proposal # 1, Transform # 9 acceptable Matches global IKE entry # 2

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing ISAKMP SA payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing ke payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing nonce payload

%PIX-7-713906: Group = MYGROUP, IP = 192.168.1.2, Generating keys for Responder...

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing ID payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing hash payload

%PIX-7-715076: Group = MYGROUP, IP = 192.168.1.2, Computing hash for ISAKMP

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing Cisco Unity VID payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing xauth V6 VID payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing dpd vid payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing NAT-Traversal VID ver 02 payload

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing NAT-Discovery payload

%PIX-7-713906: Group = MYGROUP, IP = 192.168.1.2, computing NAT Discovery hash

```

%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing NAT-
Discovery payload
%PIX-7-713906: Group = MYGROUP, IP = 192.168.1.2, computing NAT Dis-
covery hash
%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing Frag-
mentation VID + extended capabilities payload
%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing VID
payload
%PIX-7-715048: Group = MYGROUP, IP = 192.168.1.2, Send Altiga/Cisco
VPN3000/Cisco ASA GW VID
%PIX-7-713236: IP = 192.168.1.2, IKE_DECODE SENDING Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + HASH (8)
+ VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NAT-D (130)
+ NAT-D (130) + VENDOR (13) + VENDOR (13) + NONE (0) total length :
461
%PIX-7-713236: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + NOTIFY (11) + NONE (0) total length : 56
%PIX-7-713236: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + NOTIFY (11) + NONE (0) total length : 56
%PIX-5-713904: Group = MYGROUP, IP = 192.168.1.2, Received an un-en-
crypted INVALID_HASH_INFO notify message, dropping
%PIX-4-713903: Group = MYGROUP, IP = 192.168.1.2, Error, peer has in-
dicated that something is wrong with our message. This could indicate
a pre-shared key mismatch.
%PIX-4-713903: Group = MYGROUP, IP = 192.168.1.2, Information Exchange
processing failed

```

Missing IPSec VPN Client Address Pool

Determining that the IPSec client cannot connect due to a required address pool for dynamic IP address assignment being absent requires more intensive examination. The log output shown below has been truncated considerably; the actual output is some 110+ lines long! Note that a special message header, **IPAA**, is used to indicate a problem with IP Address Assignment.

```

pixfirewall(config)# %PIX-5-111008: User 'enable_15' executed the 'log-
ging on' command.
%PIX-7-609001: Built local-host outside:192.168.1.2
%PIX-6-302015: Built inbound UDP connection 12 for out-
side:192.168.1.2/500 (192.168.1.2/500) to identity:192.168.1.202/500
(192.168.1.202/500)
%PIX-7-713236: IP = 192.168.1.2, IKE_DECODE RECEIVED Message (msgid=0)
with payloads : HDR + SA (1) + KE (4) + NONCE (10) + ID (5) + VENDOR

```

```

(13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + VENDOR (13) + NONE
(0) total length : 852
%PIX-7-715047: IP = 192.168.1.2, processing SA payload
%PIX-7-715047: IP = 192.168.1.2, processing ke payload
      <output omitted>
%PIX-7-715047: IP = 192.168.1.2, processing VID payload
%PIX-7-715049: IP = 192.168.1.2, Received Cisco Unity client VID
%PIX-7-713906: IP = 192.168.1.2, Connection landed on tunnel_group MY-
GROUP
%PIX-7-715047: Group = MYGROUP, IP = 192.168.1.2, processing IKE SA
payload
%PIX-7-715028: Group = MYGROUP, IP = 192.168.1.2, IKE SA Proposal # 1,
Transform # 9 acceptable Matches global IKE entry # 2
%PIX-7-715046: Group = MYGROUP, IP = 192.168.1.2, constructing ISAKMP
SA payload
      <output omitted>
%PIX-6-113012: AAA user authentication Successful : local database :
user = doug
%PIX-6-113009: AAA retrieved default group policy (MYGROUP) for user =
doug
%PIX-6-113008: AAA transaction status ACCEPT : user = doug
%PIX-7-715019: Group = MYGROUP, Username = doug, IP = 192.168.1.2,
IKEGetUserAttributes: primary DNS = cleared
%PIX-7-715019: Group = MYGROUP, Username = doug, IP = 192.168.1.2,
IKEGetUserAttributes: secondary DNS = cleared
%PIX-7-715019: Group = MYGROUP, Username = doug, IP = 192.168.1.2,
IKEGetUserAttributes: primary WINS = 10.16.1.100
%PIX-7-715019: Group = MYGROUP, Username = doug, IP = 192.168.1.2,
IKEGetUserAttributes: secondary WINS = cleared
      <output omitted>
%PIX-7-737001: IPAA: Received message 'UTL_IP_[IKE_]ADDR_REQ'
%PIX-5-737003: IPAA: DHCP configured, no viable servers found for tun-
nel-group 'MYGROUP'
%PIX-4-737019: IPAA: Unable to get address from group-policy or tun-
nel-group local pools
%PIX-5-737007: IPAA: Local pool request failed for tunnel-group 'MY-
GROUP'
%PIX-4-737012: IPAA: Address assignment failed

```

Bad User Password and Missing Address Pool for SSL Any-Connect Client

To conclude our illustration of the use of syslog for troubleshooting VPNs, we will show a log output as an example of a “fat-fingered” password combined, again, with an absent IP address pool. Once more, considerable output of the syslog has been truncated for both clarity as well as brevity. Note that the relevant message lines for user authentication failure have AAA as an indicator. Secondly, although numerous lines of actual output were omitted, they would show that upon successful authentication, a new Transport Layer Server (TLS) SSL session is established. Once more, the absence of a configured IP Address pool has the characteristic IPAA header.

```
%ASA-6-302013: Built inbound TCP connection 1 for outside:192.168.1.2/3092 (192.168.1.2/3092) to identity:192.168.1.205/41443 (192.168.1.205/41443)
%ASA-6-725001: Starting SSL handshake with client outside:192.168.1.2/3092 for TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:192.168.1.2/3092 proposes the following 8 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-MD5
%ASA-7-725011: Cipher[2] : RC4-SHA
%ASA-7-725011: Cipher[3] : DES-CBC3-SHA
%ASA-7-725011: Cipher[4] : DES-CBC-SHA
%ASA-7-725011: Cipher[5] : EXP-RC4-MD5
%ASA-7-725011: Cipher[6] : EXP-RC2-CBC-MD5
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : EDH-DSS-DES-CBC-SHA
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client outside:192.168.1.2/3092
%ASA-6-725002: Device completed SSL handshake with client outside:192.168.1.2/3092
      <output omitted>
%ASA-6-113015: AAA user authentication Rejected : reason = Invalid password : local database : user = doug
%ASA-6-716039: Group <DefaultWEBVPNGroup> User <doug> IP <192.168.1.2> Authentication: rejected, Session Type: WebVPN.
```

```

%ASA-7-711002: Task ran for 12 msec, Process = Unicorn Proxy Thread,
PC = 8b5480d, Traceback =
%ASA-7-711002: Task ran for 12 msec, Process = Unicorn Proxy Thread,
PC = 8b5480d, Traceback = 0x08B5480D 0x08B3A17A 0x08B3BA76
0x08B3BB25 0x08B708CA 0x08B39C0E 0xD3D08418 0xD4DB1F68
%ASA-6-302013: Built inbound TCP connection 7 for out-
side:192.168.1.2/3098 (192.168.1.2/3098) to identi-
ty:192.168.1.205/41443 (192.168.1.205/41443)
%ASA-6-725001: Starting SSL handshake with client out-
side:192.168.1.2/3099 for TLSv1 session.
%ASA-6-725003: SSL client outside:192.168.1.2/3099 request to resume
previous session.
%ASA-6-725002: Device completed SSL handshake with client out-
side:192.168.1.2/3099
%ASA-6-113012: AAA user authentication Successful : local database :
user = doug
%ASA-6-113009: AAA retrieved default group policy (DfltGrpPolicy) for
user = doug
%ASA-6-113008: AAA transaction status ACCEPT : user = doug
%ASA-7-734003: DAP: User doug, Addr 192.168.1.2: Session Attribute
aaa.cisco.username = doug
%ASA-7-734003: DAP: User doug, Addr 192.168.1.2: Session Attribute
aaa.cisco.tunnelgroup = DefaultWEBVPNGroup
%ASA-6-734001: DAP: User doug, Addr 192.168.1.2, Connection AnyCon-
nect: The following DAP records were selected for this connection: Dfl-
tAccessPolicy
  %ASA-6-716001: Group <DfltGrpPolicy> User <doug> IP <192.168.1.2> We-
bVPN session started.
%ASA-6-716038: Group <DfltGrpPolicy> User <doug> IP <192.168.1.2> Au-
thentication: successful, Session Type: WebVPN.
      <output omitted>
%ASA-6-725001: Starting SSL handshake with client out-
side:192.168.1.2/3110 for TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:192.168.1.2/3110 proposes the fol-
lowing 6 cipher(s). (output continues, next page)

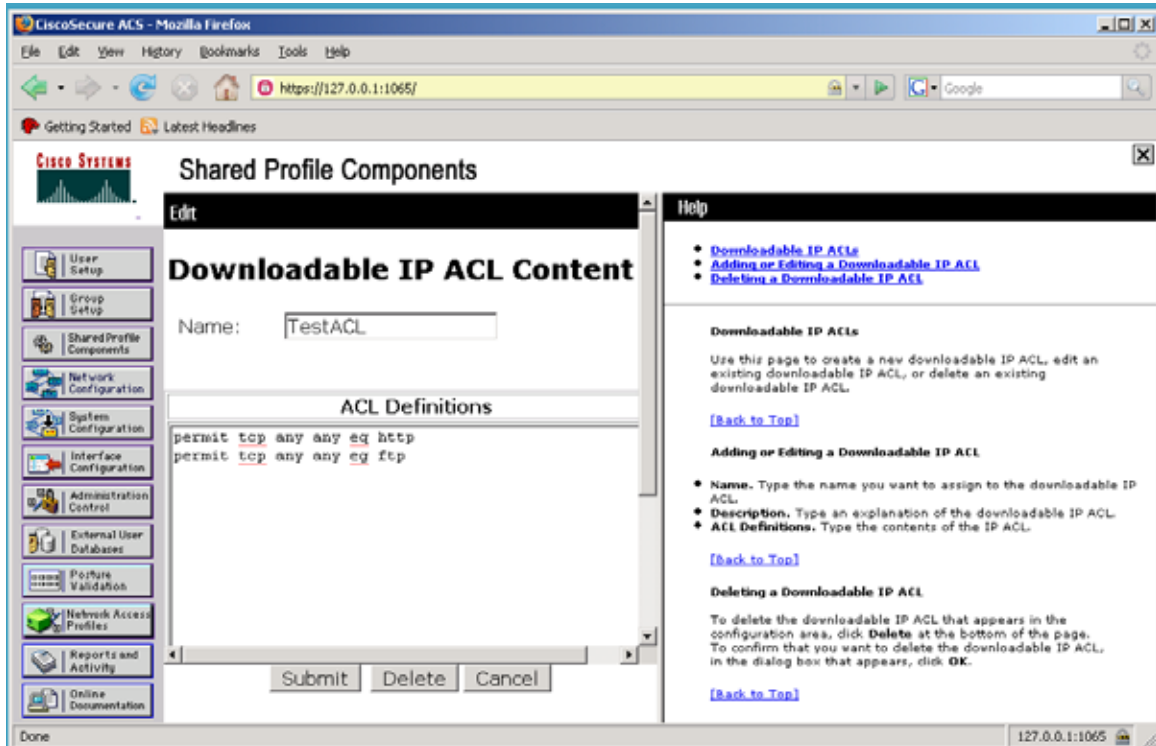
```

```
%ASA-7-725011: Cipher[1] : AES256-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : DES-CBC3-SHA
%ASA-7-725011: Cipher[4] : RC4-SHA
%ASA-7-725011: Cipher[5] : RC4-MD5
%ASA-7-725011: Cipher[6] : DES-CBC-SHA
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session
with client outside:192.168.1.2/3110
%ASA-6-725002: Device completed SSL handshake with client out-
side:192.168.1.2/3110
%ASA-7-737001: IPAA: Received message 'UTL_IP_[IKE_]ADDR_REQ'
%ASA-4-737019: IPAA: Unable to get address from group-policy or tun-
nel-group local pools
%ASA-5-737007: IPAA: Local pool request failed for tunnel-group 'De-
faultWEBVPNGroup'
%ASA-4-737012: IPAA: Address assignment failed
%ASA-3-722020: TunnelGroup <DefaultWEBVPNGroup> GroupPolicy <DfltGrp-
Policy> User <doug> IP <192.168.1.2> No address available for SVC con-
nection
%ASA-6-725007: SSL session with client outside:192.168.1.2/3110 termi-
nated.
```

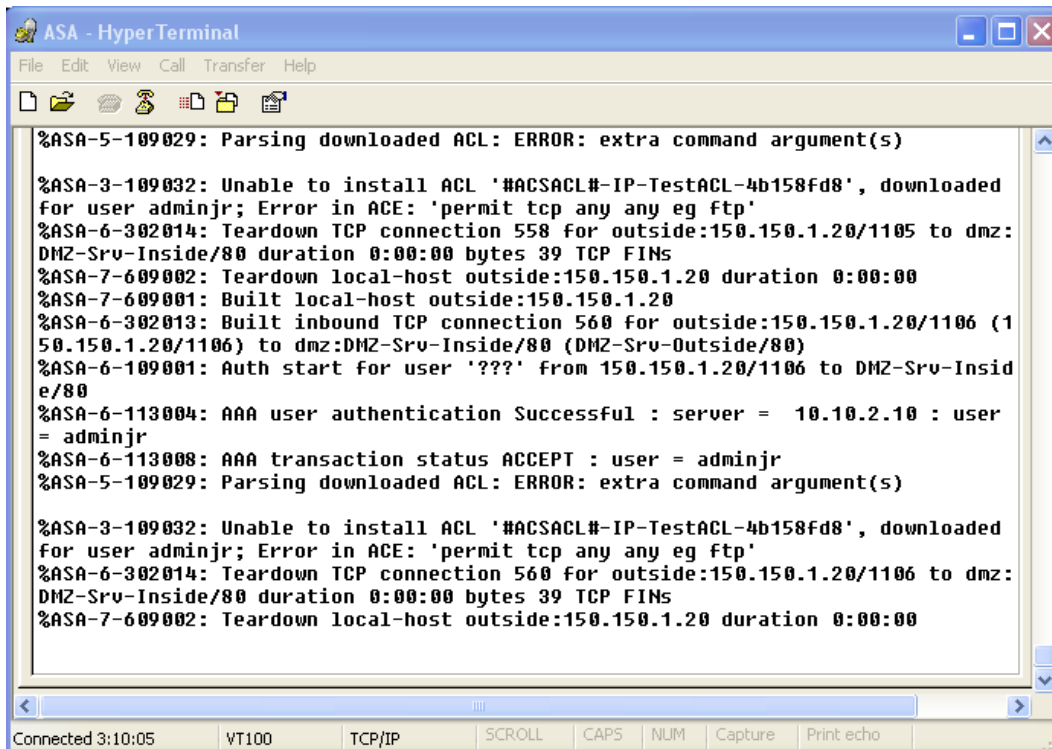
Troubleshooting Downloadable Access Lists

A very powerful feature on the ASA or PIX firewall is the capability for a dynamically downloaded user or group-specific access list in RADIUS. This can provide not only user-specific control of proxy access to applications through the security appliance but also control of access to private network resources through an otherwise unrestricted remote access VPN tunnel. This section will examine the implementation of these lists using CiscoSecure® ACS.

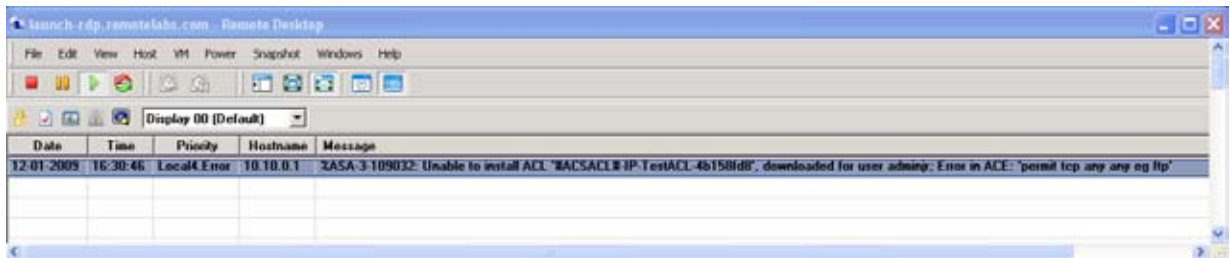
After logging into the ACS and choosing Interface Configuration Advanced Options, the Group-Level Downloadable ACLs and/or User-Level Downloadable ACLs need to be selected. Once this is done a Downloadable IP ACL can be configured under Shared Profile Components. An example is shown below with the intentional error of "eg" vs "eq" in the list.



Sadly, the CiscoSecure® ACS parser does not catch this error; instead, output from the security appliance syslog can be used to find it as shown below on the ASA console:



This can also be seen on the following output screen from Kiwi® Syslog Service Manager:



Note that both of these screenshots show the line with the error. The impact of only one bad keystroke is rather dramatic; the entire list fails the download as evidenced by the "Unable to install ACL.." message seen in the console output above.

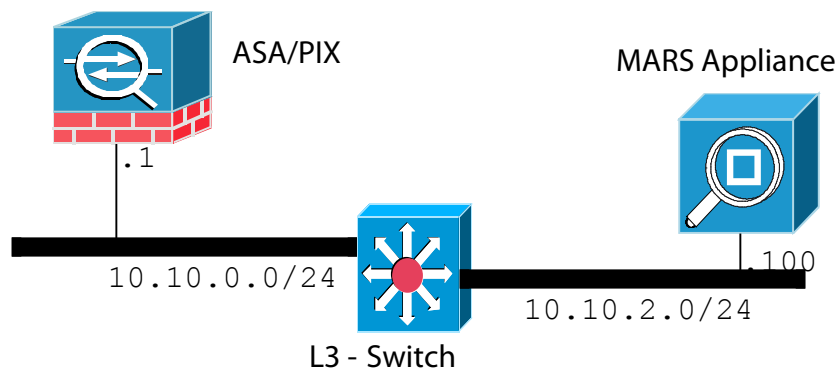
Secure Reporting Using Secure Logging with TCP and TLS

Occasionally, a network administrator may desire to send syslog output from the "outside" or Internet-facing interface of a security appliance to a remote collector. By default, the operating system offers a warning when this is attempted:

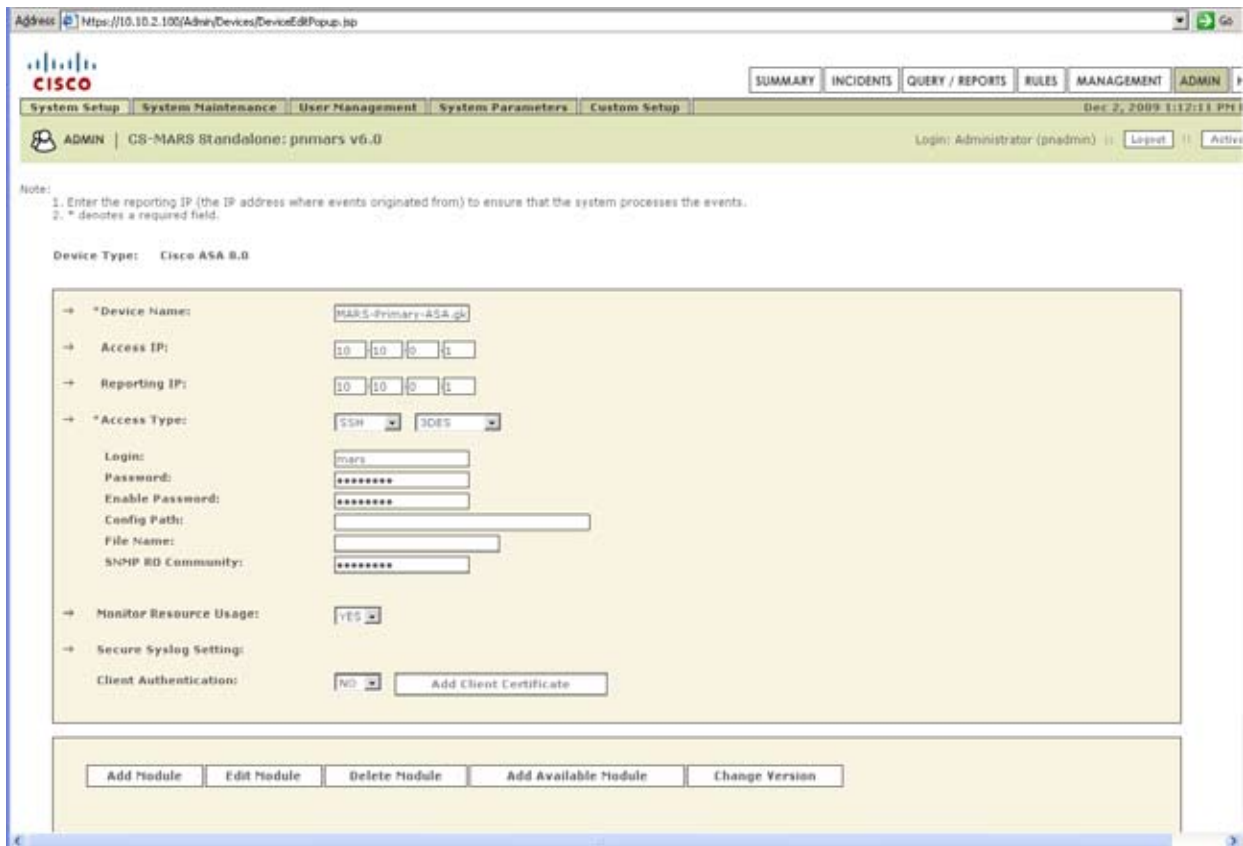
```
WARNING: interface GigabitEthernet0/0 security level is 0. (ASAOS8.x)
Warning: Sending syslogs to a non-inside interface may be insecure
(PIXOS6.3)
```

Operating System 8.0 on the PIX and ASA security appliances adds the capability to send encrypted syslog messages over to an SSL-capable collector. When the author tested this new secure logging option, it was found NOT to be an easy implementation. Troubleshooting using syslog (the subject of this paper!) was required along with the importing of an SSL certificate to make this successful.

Scenario



As required for Cisco MARS to recognize the syslog output from a device, it must be defined with the appropriate device type underneath the **ADMIN: System Setup: Security and Monitor Devices** area. A screenshot for this is shown below:



The terminal output below shows what was entered on the ASA and the ensuing problem which resulted: (Note that important certificate details are shown in **bold font**)

```
logging host inside 10.10.2.100 tcp/1470 secure
```

```
WARNING: A secure logging connection can only be established with a
        SSL/TLS capable syslog server. If a SSL/TLS connection cannot
        be established, all new connections will be denied.
```

```
This default behavior may be changed by enabling logging
permit-hostdown.
```

```
MARS-Primary-ASA(config)# %ASA-5-111008: User 'enable_15' executed the
'logging host inside 10.10.2.100 tcp/1470 secure' command.
```

```
%ASA-6-302013: Built outbound TCP connection 3371 for in-
side:10.10.2.100/1470 (10.10.2.100/1470) to NP Identity
Ifc:10.10.0.1/1054 (10.10.0.1/1054)
```

```

%ASA-6-725001: Starting SSL handshake with server inside:10.10.0.1/1054
for TLSv1 session.
%ASA-7-725009: Device proposes the following 4 cipher(s) to server in-
side:10.10.0.1/1054
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725013: SSL Server inside:10.10.0.1/1054 choose cipher : RC4-
SHA
%ASA-7-717025: Validating certificate chain containing 1 certificate(s).
%ASA-7-717029: Identified client certificate within certificate chain.
serial number: 4987A23A, subject name: cn=www.cisco.com,ou=STG CS-
MARS,o=Cisco Systems,l=San Jose,st=California,c=US.
%ASA-3-717009: Certificate validation failed. No suitable trust-
points found to validate certificate serial number: 4987A23A, sub-
ject name: cn=www.cisco.com,ou=STG CS-MARS,o=Cisco Systems,l=San
Jose,st=California,c=US.
%ASA-3-717027: Certificate chain failed validation. No suitable trust-
point was found to validate chain.
%ASA-7-725014: SSL lib error. Function: SSL3_GET_SERVER_CERTIFICATE
Reason: certificate verify failed
%ASA-7-710005: TCP request discarded from MARS-Inside/1470 to in-
side:10.10.0.1/1054
%ASA-6-302014: Teardown TCP connection 3371 for inside:MARS-In-
side/1470 to NP Identity Ifc:10.10.0.1/1054 duration 0:00:00 bytes 63
TCP Reset-I

```

As will be shown next, the information in the above output containing the SSL certificate serial number is critical to the successful operation of Secure Logging with TCP/TLS. These are shown in the output above in **bold** font. Here are the steps taken to solve this problem:

- 1) Go to **ADMIN: System Maintenance: Certificates** in the Cisco MARS® GUI; copy this Base64 encoded certificate to Notepad.
- 2) Open a CLI session to the ASA, get into config mode and generate an RSA key pair:

```

ciscoasa(config)# crypto key generate rsa label <key-name> modulus
1024

```

3) Configure the trustpoint:

```
ciscoasa(config)# crypto ca trustpoint <trustpoint-name>
ciscoasa(config-ca-trustpoint)# subject-name <Enter cert details
here>
ciscoasa(config-ca-trustpoint)# keypair <key-name>
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)# exit
```

4) Authenticate the trustpoint: (both a CA cert and an SSL cert are self-signed)

```
ciscoasa(config)# crypto ca authenticate trustpoint <trustpoint-
name>
```

Enter the base 64 encoded CA certificate.

End with the word "quit" on a line by itself **(sample shown here)**

-----BEGIN CERTIFICATE-----

```
MIICaDCCAdECBEmHojowDQYJKoZIhvcNAQEEBQAwezELMAkGA1UEBhMCVVMx-
EzARBgNVBAgTCkNhbg1mb3JuaWEwETAPBgNVBACtCFNhb3N1MRYwFAYD-
VQKQEW1DaXNjbyBTeXN0ZW1zMRQwEgYDVQQLewtTVEcgQ1MtTUFSUzEWMBQ-
GA1UEAxMNd3d3LmNpc2NvLmNvbTAeFw0wOTAyMDMwMTQ3MzhaFw0yNDAxMzEw-
MTQ3MzhaMHsxCzAJBgNVBAYTAlVTMRMwEQYDVQQLIEwpcDYWxpZm9ybmlhMREwDwYD-
VQHEhwTYW4gSm9zZTEwMBQGA1UEChMNQ2l2Y28gU3lzdGVtczEUMBIGA1UECx-
MLU1RHIENTLU1BULMxYjAUBgNVBAMTDXdy5jaXNjby5jb20wgZ8wDQYJKoZI-
hvcNAQEBBQADgY0AMIGJAoGBAM42YRrHGodydD0R4++OLJ+RibVTv2jgUIvUG1T
q4+yD0TrSzUUtFbn/4DAR1II0r6xkxsjv8JlnnFIVn+j1JurnoOgb4oh0wPzqTC
2PMGSpXjpZvIt8vksIxX+tX2WSfm3t2ngQ/kxmvTJm6Euz3kti8qRgNdY/2lOe
vZuqkYljAgMBAAEwDQYJKoZIhvcNAQEEBQADgYEApS41l0vdhrSn/z1d7eAxI-
JHaoIqvYkoz9aKGFYNJLaYZItNBqaE7pzeVGuK6Q5XsUEOV2DOrNcLBlqaPK/
fC/+THmnYr0lTMCCZomnYQu/r4RD4P2JjJYXlmFVYJMtM481IV6pGJ2aVHeW9O5M-
QsU/EqcWgV7Bs7BwmlKfhrQUE=
```

-----END CERTIFICATE-----

quit

Once the above steps have been taken, the successful logging of messages with TCP/TLS can be verified several ways. First, here is the result of a "show conn all" command from the ASA; the "all" option is necessary to show connections to/from the ASA itself:

```
MARS-Primary-ASA# show conn all detail
```

```
4 in use, 20 most used
```

```
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,  
      B - initial SYN from outside, C - CTIQBE media, D - DNS, d - dump,  
      E - outside back connection, F - outside FIN, f - inside FIN,  
      G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,  
      i - incomplete, J - GTP, j - GTP data, K - GTP t3-response  
      k - Skinny media, M - SMTP data, m - SIP media, n - GUP  
      O - outbound data, P - inside back connection, q - SQL*Net data,  
      R - outside acknowledged FIN,  
      R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,  
      s - awaiting outside SYN, T - SIP, t - SIP transient, U - up, W - WAAS,  
      X - inspected by service module
```

```
TCP inside: 10.10.2.100/1470 NP Identity Ifc:10.10.0.1/1064 flags UO
```

Here is the result of "show logging" on the ASA:

```
MARS-Primary-ASA# show logging
```

```
Syslog logging: enabled
```

```
  Facility: 20
```

```
  Timestamp logging: disabled
```

```
  Standby logging: disabled
```

```
  Deny Conn when Queue Full: disabled
```

```
  Console logging: disabled
```

```
  Monitor logging: disabled
```

```
  Buffer logging: disabled
```

```
  Trap logging: level debugging, facility 20, 6690 messages logged
```

```
    Logging to inside 10.10.2.100 tcp/1470 SECURE
```

Previously the word "disabled" was next to the SECURE word above in the output when the certificate verification had failed.

Secure logging is confirmed further by observing Real-Time Query log messages in MARS®:

The screenshot shows the Cisco MARS Query/Reports interface. The top navigation bar includes 'SUMMARY', 'INCIDENTS', 'QUERY / REPORTS', 'RULES', 'MANAGEMENT', and 'ADMIN'. The current page is 'QUERY / REPORTS' for 'CS-MARS Standalone: pmrars v6.0'. The user is logged in as 'Administrator (phadmin)'. The query type is 'Event Raw Messages ranked by Time, Real Time (raw events)'. The query criteria table is as follows:

Source IP	Destination IP	Service	Events	Device	Reported User	IPS Risk Rating	IPS Threat Rating	Keyword	Operation	Rule	Action
ANY	ANY	ANY	ANY	MARS-Primary-ASA.gkl.local	ANY	ANY	ANY	ANY	None	ANY	ANY

The 'Query Results' section displays a table with the following data:

Event ID	Event Type	Time	Reporting Device	Raw Message
203263	Built/teardown/permitted IP connection	Dec 2, 2009 1:04:24 PM PST	MARS-Primary-ASA.gkl.local	<166>%ASA-6-302016: Teardown UDP connection 3529 for outside:TIME.NIST.GOV/123 to inside:10.10.1.10/4524 duration 0:02:02 bytes 96
203264	Firewall user entered a command that did not modify the config	Dec 2, 2009 1:04:43 PM PST	MARS-Primary-ASA.gkl.local	<167>%ASA-7-111009: User 'enable_15' executed cmd: show logging
203265	Built/teardown/permitted IP connection	Dec 2, 2009 1:04:43 PM PST	MARS-Primary-ASA.gkl.local	<166>%ASA-6-302015: Built outbound UDP connection 3550 for outside:TIME.NIST.GOV/123 (TIME.NIST.GOV/123) to inside:L3-SWITCH/123 (209.200.1.56/123)
203267	Built/teardown/permitted IP connection	Dec 2, 2009 1:04:57 PM PST	MARS-Primary-ASA.gkl.local	<166>%ASA-6-302015: Built inbound UDP connection 3551 for inside:MARS-Inside/2606 (MARS-Inside/2606) to NP Identity Ifc:10.10.0.1/161 (10.10.0.1/161)
203268	TCP or UDP access permitted to the	Dec 2, 2009 1:04:57 PM PST	MARS-Primary-ASA.gkl.local	<167>%ASA-7-710002: UDP access permitted from MARS-Inside/11786 to inside:10.10.0.1/snmp

Summary

The reader should particularly note that for all of the preceding syslog examples shown, the log level was chosen to be at the **debug** level for both the console as well as the syslog server. In a production environment, logging to this trivial level of detail is frequently not an option; the huge amount of real-time output would make the console terminal virtually unusable. Instead, what should be considered upon looking at the examples above would be changing the level of the 6-digit syslog message IDs for “interesting” messages shown above, so that a more suitable log level (**warnings**, for example) could be chosen. This will result in a more manageable number of messages.

As seen above, syslog provides both an effective and secure (if using TLS) mechanism for providing meaningful auditing and troubleshooting information for a network administrator. The decision to implement a fully functional syslog collector (like Cisco MARS) is highly recommended.

Learn More

Learn more about how you can improve productivity, enhance efficiency, and sharpen your competitive edge. Check out the following Global Knowledge courses:

[IINS – Implementing Cisco® IOS Network Security](#)

[SNRS – Securing Networks with Cisco® Routers & Switches v3.0](#)

[SNAF – Securing Networks with ASA Fundamentals](#)

[SNAA – Securing Networks with ASA Advanced](#)

MARS – Cisco® Monitoring, Analysis, and Response System v3.0

CANAC – Implementing NAC Appliance (formerly Cisco® Clean Access)

CCNA-TS - Troubleshooting Cisco Internetworking for Network Associates

For more information or to register, visit www.globalknowledge.com or call 1-800-COURSES to speak with a sales representative. Our courses and enhanced, hands-on labs offer practical skills and tips that you can immediately put to use. Our expert instructors draw upon their experiences to help you understand key concepts and how to apply them to your specific work situation. Choose from our more than 1,200 courses, delivered through Classrooms, e-Learning, and On-site sessions, to meet your IT and business training needs.

About the Author

Douglas B. McKillip, P.E., CCIE #1851, is the President and Principal Consultant of Innovative Integrators Incorporated, a Delaware Corporation actually based in Delaware. In addition to a BS and MS in Chemical Engineering from M.I.T., Doug also later obtained an M.S. from the University of Delaware in Computer and Information Science. After 15 years of experience at DuPont and a brief stint with the original startup company associated with the Raptor Eagle™ Firewall, Doug began his now 15+ year career of teaching and consulting, specializing in Internet Security with hardware from Cisco® since 1998. He can be reached at innovativeint@mindspring.com.