Ministry of Information & Communications Technology

وزارة الاتصالات و تكنولوجيا المعلومات.

Guidelines for Incident Management “Pre-requisite Measures”

“How to be prepared to handle a computer incident”

Document Control

Version:	1.0
Author:	Cyber Security Division - MICT
Classification:	Public
Date of Issue:	April 2014

Contents

Introduction

Information Technology has steadily risen from being a business enabler to be a business driver. As organizations and businesses increase their dependence on information technology and we move towards a knowledge-based economy, it is imperative that we safeguard this knowledge.

The safeguard strategy revolves around the ability to prevent an incident from happening, respond in case of an incident and be able to recover from an incident.

A key dimension of this protection strategy is the ability of an organization to monitor the system in an adequate manner. The monitoring consists of two parts:

Adequate Logging of active systems in the infrastructure (Network, System, Applications etc)

Monitoring the logs

This document intends to provide guidance to IT administrators, operators, and security practitioners on building a log management system and the kind of logs and events that should be logged so that they may be useful in detecting, reacting or investigating an incident.

Objective

Provide necessary guidance to increase and improve the incident handling readiness, ensure that systems are ready, and provide the necessary logs and information during an incident investigation

Scope

All organizations having an IT infrastructure.

Legal Mandate

Article 14 of Decree Law No. 16 of 2014 setting the mandate of Ministry of Information and Communications Technology (hereinafter referred to as “MICT”) provides that MICT has the authority to supervise, regulate and develop the sectors of Information and Communications Technology (hereinafter “ICT”) in the State of Qatar in a manner consistent with the requirements of national development goals, with the objectives to create an environment suitable for fair competition, support the development and stimulate investment in these sectors; to secure and raise efficiency of information and technological infrastructure; to implement and supervise e-government programs; and to promote community awareness of the importance of ICT to improve individual’s life and community and build knowledge-based society and digital economy.

Article (14) of Emiri Decree No. 27 of 2014 stipulated the role of the Ministry in protecting the security of the National Critical Information Infrastructure by proposing and issuing policies and standards and ensuring compliance.

Article (15) of Emiri Decree No.27 of 2014 stipulates that the Ministry build and enable incident response framework and enhance capabilities to detect and analyze malicious content.

This Policy Document has been prepared taking into consideration current applicable laws of the State of Qatar. In the event that a conflict arises between this document and the laws of Qatar, the latter, shall take precedence. Any such term shall, to that extent be omitted from this Policy Document, and the rest of the document shall stand without affecting the remaining provisions. Amendments in that case shall then be required to ensure compliance with the relevant applicable laws of the State of Qatar.

General

In the unfortunate instance of an incident, the biggest challenge for incident handlers / investigators is the ability to visualize and reconstruct the incident. How did the attacker breach the IT infrastructure, when did the breach happen, how was the attack carried out, what information / assets were breached during the incident etc.

In order to, effectively carry out the challenge the IH team needs access to certain information such as Network design. System documentation, logs from affected systems etc.

Following are a list of recommendations and best practices collated together to help organizations prepare themselves and their abilities to handle an incident.

Documentation

A key step in managing an incident is the ability to understand possible attack vectors, attack propagation route etc. A lot of these information can be gained by understanding the IT Architecture of the affected organization. Documents such as Network Design, System Architecture, Operating systems used, configurations can shed a lot of light on possible attack vectors and how the attack propagated inside the system. A copy of configurations (especially the firewalls and routers) can shed light if the network segments were isolated and secured or if there was free flow of information.

Following is a tentative list of documents that an organization should keep updated, secured and available at all times.

- ✓ Detailed Network Diagram (With Updated IP Schema)
- ✓ Detailed System Architecture
- ✓ Schedule of OS Updates / Patches applied
- ✓ Detailed configuration of all network / security appliances (Perimeter, DMZ and Internal)
- ✓ Updated Change Management records
- ✓ If Possible AD objects Rights matrix (details of AD objects with rights assigned, especially those with admin or special privileges)
- ✓ BCP and IT DR Plans
- ✓ Updated List of IT policies and procedures
- ✓ Updated List of IS policies and procedures
- ✓ Contact details of key personnel within and outside the organization. These include Management, National CERT (Q-CERT), Law enforcement Agencies.
- ✓ If possible, procedures related to such external organizations. It will help if the organization is aware on how and when to reach out to such organizations during an incident to reduce the chaos during an incident.

Logging Infrastructure

Following is a brief guidance to build an effective log management system and be able to collect the right logs that can add value in the process of detecting and responding to an incident.

Building an effective Log management system and the right processes around it to monitor these logs is a key step in building an effective incident response capability.

Log Management System:

1. Collect logs from all active devices on an independent centralized log server.
2. The system should ideally be non-proprietary and be able to handle logs from multiple systems and formats.
3. Centralized logging provides the following advantages:
   - ✓ Single system, easy maintenance and operation
   - ✓ Ability to co-relate events and have a birds eye-view on the system
4. Where possible, enable multiple logging such as syslog logging, buffered logging and SNMP etc.
5. For SNMP use v3 or the latest secured version.

File Requirements:

1. When events are logged in to a file, a process should be in place to conduct housekeeping on such files.
2. Circular logging or overwrite by default should be disabled so as to ensure that logs are not over written.
3. Identify and maintain an optimum file size based on the OS and file reader capabilities.
4. Rotate files at regular intervals.

Disk Requirements:

Consider Disk / Storage requirements as one of the key aspects in the design of log management system. Logs can be huge, primarily influenced by the following factors:

- ✓ Infrastructure size: Number of active elements that generate logs.
- ✓ Level of logging: Based on the level of logs that is configured. A Debug level will generate much more logs than an Information level.
- ✓ Log Retention Period: The amount of time for which the logs are to be retained.
- ✓ Storage Design: Organizations might choose to have a strategy wherein they might split the amount of logs available online:
  - o Short Term: Available online
  - o Long Term: Backups

Time Synchronization:

Accurate time stamping is a key requirement for a log management system and is vital in co-relating logs from different system during an incident investigation.

1. Synchronize all the hosts / active devices on the network to a single reliable time source.

Log Retention:

Perform due diligence to understand and identify for how long the logs should be retained. It might be appropriate to consult the Legal department for their advice on the matter.
The following factors influence the Log retention period:

- ✓ Legal requirements
- ✓ Regulatory requirements
- ✓ Organizational requirements

*NIA Policy recommends logs retention for a period of 90 days.

Access Control & Security:

As per the NIA Policy, classify all security logs as C3 – Confidential. It is imperative that the log management system is secured accordingly to protect these critical information.

1. The logging machine should be hardened as per the best practices.
2. Enable adequate auditing on the system to monitor privilege actions such as deleting of logs.
3. The log management system (LMS) should be on a separate trusted and protected vlan network.
4. Each operators should have their unique login credential to access the LMS.
5. Access to the LMS should be restricted to NOC / SOC operators on a Need to Know basis.

Log monitoring:
The most important and probably the weakest element is Log monitoring as it involves human involvement.

1. Define a process and allocate adequate resources to monitor logs. Based on the criticality of business, the monitoring could 24x7 or business hours.
2. Make use of technology as much as possible to alleviate the pain points:
    a. Use co-relation of Events / Logs to have a bird eye-view on what is happening in your network /system.
    b. Configure system to send automated alerts, for certain marked / pre-defined activities.
    c. Provide automated responses. When any anomaly is detected, system can alert the administrators of the activity as well as perform automated responses. For example, in the rules that detect an external attack, a script can be run in response to that attack and the administrators can be emailed and/or paged with details of what happened.
3. Revisit the rules defined for collecting and processing logs from time to time in consideration of changing threat scenarios.
4. Define a process to escalate an incident.

* Refer to NIA Policy v2.0 for comprehensive security requirements.

Logs / Events

A key question during the design of a Log management system in place is, “What events should I Log?”.

The level and content of security monitoring, alerting and reporting needs to be set during the requirements and design stage and should address your potential threats and measure up to your risk appetite.

There is no silver bullet solution to this problem, and although it might be tempting to log everything, the approach can lead to a deluge of logs. Besides the issues of managing the size of such logs in terms of storage, network bandwidth, the challenge would be in being able to find real problems.

Nevertheless, we should still log where possible the following events:

1. Input validation failures e.g. protocol violations, unacceptable encodings, invalid parameter names and values
2. Output validation failures e.g. database record set mismatch, invalid data encoding
3. Authentication successes and failures
4. Authorization failures

5. Session management failures e.g. cookie session identification value modification
6. Application errors and system events e.g. syntax and runtime errors, connectivity problems, performance issues, third party service error messages, file system errors, file upload virus detection, configuration changes
7. Application and related systems start-ups and shut-downs, and logging initialization (starting and stopping)
8. Use of higher-risk functionality e.g. network connections, addition or deletion of users, changes to privileges, assigning users to tokens, adding or deleting tokens, use of administrative privileges, access by application administrators, access to payment cardholder data, use of data encrypting keys, key changes, creation and deletion of system-level objects, data import and export including screen-based reports, submission of user-generated content - especially file uploads
9. Legal and other opt-ins e.g. permissions for mobile phone capabilities, terms of use, terms & conditions, personal data usage consent, permission to receive marketing communications

Optionally consider if the following events can be logged and whether it is desirable information:

1. Sequencing failure
2. Excessive use
3. Data changes
4. Fraud and other criminal activities
5. Suspicious, unacceptable or unexpected behavior
6. Modifications to configuration
7. Application code file and/or memory changes

Log / Event attributes

Once you have identified the types of events and the level of logs that will be collected, it is essential to ensure that each log entry includes sufficient information for the intended subsequent monitoring and analysis. It could be full content data, but is more likely to be an extract or just summary properties. The application logs must record "when, where, who and what" for each event. The properties for these will be different depending on the architecture, class of application and host system/device, but often include the following:

1. When
    a. Log date and time (international format)
    b. Event date and time - the event time stamp may be different to the time of logging e.g. server logging where the client application is hosted on remote device that is only periodically or intermittently online
    c. Interaction identifier [Note A]

2. Where
    a. Application identifier e.g. name and version
    b. Application address e.g. cluster/host name or server IPv4 or IPv6 address and port number, workstation identity, local device identifier
    c. Service e.g. name and protocol
    d. Geolocation
    e. Window/form/page e.g. entry point URL and HTTP method for a web application, dialogue box name
    f. Code location e.g. script name, module name
3. Who (human or machine user)
    a. Source address e.g. user's device/machine identifier, user's IP address, cell/RF tower ID, mobile telephone number
    b. User identity (if authenticated or otherwise known) e.g. user database table primary key value, user name, license number
4. What
    a. Type of event [Note B]
    b. Severity of event [Note B] e.g. {0=emergency, 1=alert, ..., 7=debug}, {fatal, error, warning, info, debug, trace}
    c. Security relevant event flag (if the logs contain non-security event data too)
    d. Description

Additionally consider recording:

1. Secondary time source (e.g. GPS) event date and time
2. Action - original intended purpose of the request e.g. Log in, Refresh session ID, Log out, Update profile
3. Object e.g. the affected component or other object (user account, data resource, file) e.g. URL, Session ID, User account, File
4. Result status - whether the ACTION aimed at the OBJECT was successful e.g. Success, Fail, Defer
5. Reason - why the status above occurred e.g. User not authenticated in database check ..., Incorrect credentials
6. HTTP Status Code (web applications only) - the status code returned to the user (often 200 or 301)
7. Request HTTP headers or HTTP User Agent (web applications only)
8. User type classification e.g. public, authenticated user, CMS user, search engine, authorized penetration tester, uptime monitor (see "Data to exclude" below)

9. Analytical confidence in the event detection [Note B] e.g. low, medium, high or a numeric value
10. Responses seen by the user and/or taken by the application e.g. status code, custom text messages, session termination, administrator alerts
11. Extended details e.g. stack trace, system error messages, debug information, HTTP request body, HTTP response headers and body
12. Internal classifications e.g. responsibility, compliance references
13. External classifications e.g. NIST Security Content Automation Protocol (SCAP), Mitre Common Attack Pattern Enumeration and Classification (CAPEC)

Note A: The "Interaction identifier" is a method of linking all (relevant) events for a single user interaction (e.g. desktop application form submission, web page request, mobile app button click, web service call). The application knows all these events relate to the same interaction, and this should be recorded instead of losing the information and forcing subsequent correlation techniques to re-construct the separate events. For example a single SOAP request may have multiple input validation failures and they may span a small range of times. As another example, an output validation failure may occur much later than the input submission for a long-running "saga request" submitted by the application to a database server.

Note B: Each organisation should ensure it has a consistent, and documented, approach to classification of events (type, confidence, severity), the syntax of descriptions, and field lengths & data types including the format used for dates/times.

System Preparation:

Operating System

1. Log system startup and shutdown events
2. Log start and stop of services (success and failure)
3. Log installation and uninstallation of programs, devices, services etc. (success and failure)
4. Log access of users (success and failure)
5. Log privilege users and their activities (success and failure)
6. Log user privilege escalations(success and failure)
7. Log resource utilization (e.g. CPU, Memory, Disk etc)

DHCP

1. Log the following DHCP events:
    a. Start and Stop of services
    b. New IP address leased to a client
    c. Renew / Release of a leased IP by a client
    d. IP address in use on network
    e. Errors, e.g. Scope exhaustion
    f. DNS Dynamic update request
    g. Status of DNS Dynamic update request
2. DHCP Server authorization event and any associated success / failures / errors

DNS

1. Log the following activities in a DNS
    a. Application – Logs from DNS servers related to the application itself such as the start of a zone transfer between two DNS servers.
    b. DNS – Logs that indicate a query from a DNS name to an IP address or vice versa have occurred. Queries for DNS names that have failed are also typically logged to this category.
    c. Error – Any logs related to the DNS application that indicate an error.
    d. Startup – Any logs from a DNS appliance or DNS service that indicate a reboot, restart, or service availability.

Access Management / Identity Management

1. Log login attempts of all users including remote logins. (Success / Failure)
2. Configure alerts for any activity detected for dormant accounts
3. Log escalation of user privilege. (Success / Failure)
4. Unless authorized, log multiple logins from same account.
5. Log events related to provisioning of objects / users within a Directory. (Success / Failure)
6. Log information related to identity mapping actions (creation, deletion, update) that are associated with a user consent to federate.
7. Log information related to trust server actions. Examples of some trust server action are validation of a token, issuance of a token, mapping of an identity, or authorization of a Web service call.
8. Log events related to key / token management in multi factor authentication.
9. Log errors / events related to Directory management (Active Directory / Open Directory etc)
10. Logs event related to passwords (Change / Failure etc)

Firewalls

1. Log packets which are denied by the firewall filter.
2. Log rejected IP addresses.
3. Log successful and unsuccessful logins.
4. Log outbound activity from internal servers.
5. Log Source routed packets. Source routed packets may indicate that someone is trying to gain access the internal network.
6. Log traffic that is permitted across the perimeter. This includes all permitted traffic, regardless of direction (egress as well as ingress). At a minimum log header information for the first packet in a session.
7. Log firewall activities such as:
   a. Change of configuration (other than access rules e.g. change of IP address, syslog options etc.)
   b. Change of access rules
   c. Start / Shutdown of services / firewall
   d. Access Control / Login (Success / Failure)
8. Ideally, enterprises should log both "allow" and "deny" actions, but resource constraints may limit logging to "deny" actions. In such cases, enhance monitoring by use of egress filters. Further if you are running a tool such as NTOP on your perimeter, collecting RMON or Netflowdata, than it is OK not to log dropped packets as you can collect this information through other means.

VPN

1. End User Devices (EUD) shall generate logs and send to a log server.
2. Each VPN Gateway shall log when a VPN tunnel is established and terminated
3. Log all actions involving identification and authentication.
4. Log all actions performed on the audit log (off-loading, deletion, etc.
5. Log attempts to perform an unauthorized action (read, write, execute, delete, etc.) on an object.
6. Log all actions performed by a user with super privileges.
7. Log any escalation of user privileges.
8. Log certificate operations including generation, loading, or revoking of certificates.
9. Log all built-in self-test results, which may indicate failures in cryptographic functionality.
10. Log the user and role identification for role based events.
11. Log and alert immediately when the same device certificate establishes two or more simultaneous connections.

Routers / Switches

1. Log all authentication and authorization events (both success and failed attempts)
2. Log remote access to the devices
3. Log user privilege escalations
4. Log configuration changes and reboots
5. Log receipt of traffic that violates access lists
6. Log changes in interface and network status
7. Log router cryptographic security violations
8. Some event data should be maintained locally to the router.
9. Log data for all Interactive Commands
10. Log both inbound and outbound spoofing attempts.

11. Configure key ACLs to record access violations. Recommended ACL logging includes:
    a. – Antispoofing violations
    b. – VTY access attempts
    c. – HTTP access attempts
    d. – SNMP access attempts
    e. – Route filter violations
    f. – ICMP violations
    g. – Any other important filters
12. Log information on system events and user sessions.
13. Log port security violations
14. Log port status (Up/DOWN)
15. Log Vlan / Trunk status
16. Log status of specific services running on device such as routing, firewall etc

Application Gateways

1. Log connections permitted by firewall rules.
2. Log connections denied by firewall rules.
3. Record denied rule rates / frequency.
4. Log admin / superuser activity, including firewall user authentication and command usage.
5. Log end users authentication through Cut-through-proxy.
6. Log Bandwidth usage.
7. Log Protocol usage.
8. Log alerts from special features; such as Intrusion Detection System (IDS) activity, content filters etc.
9. Log Address translation (Network Address Translation (NAT) or Port Address Translation (PAT)).

Email Servers

1. Define appropriate level of diagnostic logging to be enabled
2. Enable logs related to Message Tracking to monitor flow of messages
3. Maintain and Secure the Transaction log files.
4. Disable circular logging of log files (MS Exchange)
5. Log protocols such as SMTP / POP / IMAP etc
6. Log services such as HTTP, NNTP etc
7. Log user authentication.
8. Log user privilege escalations.
9. Log access of mailboxes by non-primary users. E.g. Access of mailbox by administrator
10. Log system usage and health statistics. E.g. CPU, network traffic, Memory etc

Web Servers

1. Establish different log file names for different virtual web sites that may be installed as part of a single physical web server.
2. Define appropriate level of logging and auditing.
3. Use log file rotation as applicable.
4. Log all errors related to the application, system etc
5. Log all access requests to the web server.
6. Log entries for both successful and failed webserver requests.

Databases

1. Define appropriate level of logging and auditing.
2. Possible candidates for events to be logged to the database include:
    a. DB instances shutdown / start
    b. Transactions making changes to persistent data
    c. Transactions crossing component boundaries
    d. Access to Sensitive Data (Successful/Failed SELECTs)
    e. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)
    f. Data Changes (DML) (Insert, Update, Delete)
    g. Changes to the structure of data (such as dropping a table)
    h. Changes to data values (such as updating or inserting data)
    i. Logging database changes as far as inserts/deletes/updates,
    j. Dispatching of messages to the user
    k. Events involving financial transactions
    l. State changes to business entities
    m. Security Exceptions (Failed logins, SQL errors, etc.)
    n. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)
    o. Changes in authorization IDs
    p. Results of GRANT statements and REVOKE statements
    q. Mapping of Kerberos security tickets to IDs
    r. Access attempts by unauthorized IDs
    s. Errors and exceptions
3. Besides this some other information that should be logged include
    a. System Information

Appendices

A - Helpful Tips to Log and Monitor your Network

1. There is no “single right way” to segregate log entries. It is all about how you personally spot unsuspected patterns. You can sort by IP address, port number, or whatever info you have to work with in your logs.
2. Reviewing log files:
    a. Identify which log entries would go in which sort file. For example, a TCP reset in an HTTP stream could go in both an “error” file and an “HTTP” file. Each would make it easier to spot different types of patterns.
    b. Start by pulling our error packets (TCP resets, ICMP type 3’s & 11’s). They always indicate something is broke or someone did something unexpected.
    c. Be aware, a smart attacker / attack will not always make to your “Top 20 communicators” list. Some infected systems make as few as four outbound connections in a day.
    d. Make a note of the average size of each of your daily sort files. A sharp spike in traffic may warrant further investigation.
    e. Sometimes it is helpful to parse the same pattern into two different files. For example, you could create an “outbound HTTP” file, and then parse out all of the traffic generated during non-business hours. This would make it much easier to find infected systems calling their CnC servers. Whitelist known patch sites like Microsoft, Adobe, Anti Virus to suppress false flags.
    f. Segregate traffic based on security zone. In an ideal world, every traffic pattern you find should be described in your organization’s network usage policy. If it is not, then further investigation may be required.
    g. Look for suspicious outbound connections. For example, outbound connections coming from your public Web server could be an indication that an intruder is launching an attack against someone else from your Web server.
    h. Look for probes to ports that have no application services running on them. Before hackers try to install backdoor Trojan horse programs, they usually try to determine whether you are already using the ports these programs use. When you see many probes to some oddball port number, you can compare the number against well-known hacker programs and see if it has a hacker Trojan associated with it. For example, many probes to port 31337 might mean that someone is getting ready to try to install Back Orifice on your network.
    i. Malware can leverage any socket to call home, but most use TCP/80 (HTTP) or TCP/443 (HTTPS). This is because Malware authors know most firewall administrators do not log these outbound sessions because they are responsible for the greatest portion of perimeter traffic. If you permit this traffic to pass your perimeter, it might be a good idea to log it.
3. Tweak your scripts over time, as networks are an evolving entity and threat vector keeps changing.
4. In situations where you are logging all "allow" actions, implement supporting processes, which would allow for the efficient and timely analysis of the logs. Analysis activities should include reputation-based matching, as well as monitoring for traffic deviations.

B - Evidence Preservation – Network Devices

1. If you must get your network device functional as quickly as possible, it is vitally important that you record any volatile information that may be lost upon reconfiguration or reboot of the network device.
2. Before you make any changes to, shut down, or reboot the network device, follow these steps to gather as much of this volatile evidence as possible:
    a. Connect to the network device's console port. This is the least-intrusive way to access the network device. It does not require network access and will not tip off your attackers if they are sniffing your network.
    b. Configure your terminal emulation software to record your session.
    c. Log in to the network device and enter in to the configuration mode.
    d. Note down the current date and time.
    e. Write down the time from a trusted time source (atomic clock, NTP server, etc.) if your devices; are not synchronized to a single time source.
    f. Note the OS version, uptime, and hardware information.
    g. Note the current running configuration in memory.
    h. Note the current startup / saved configuration.
    i. Note the routing tables.
    j. Note the ARP tables.
    k. Note who is logged in.
    l. Note current logs.
    m. Note current interface configuration.
    n. Note TCP connections.
    o. Note open sockets.
    p. Note NAT translations.
    q. Note CEF forwarding table.
    r. Note SNMP v3 users.
    s. Note SNMP v3 groups.
    t. Note date and time again (Note clock detail).
    u. Write down the time from a trusted time source again.
3. Disconnect from the network device and end the terminal recording session.
4. Print out your recording session.
5. Write the two times you recorded from the trusted time source on the printout.
6. Sign and date the printout.
7. Get a witness to sign and date the printout.
8. Keep both the electronic copy and the hardcopy in a secure location until you can turn them over to law enforcement.

Next, you need to gather information from the network device externally:

1. Port scan the network device from an external system.
2. Record the time of the port scan from a trusted time source.
3. Print out the port scan and write the time on the printout.
4. If the network device is running SNMP, get a copy of the current SNMP tree. This can be done with a command such as snmpwalk (from NetSNMP http://net-snmp.sourceforge.net).
5. Record the time of the SNMP walk from a trusted time source.
6. Print out the SNMP tree info and write the time on the printout.
7. Sign and date both printouts.

8. Get a witness to sign and date both printouts.
9. Keep all copies in a secure location until you can turn them over to law enforcement.

C - Syslog Levels

Number	Keyword	Message Examples
0	Emergencies	System is unusable
1	Alerts	Immediate action needed
2	Critical	Critical conditions
3	Errors	Error conditions
4	Warnings	Warning conditions
5	Notifications	Exit global configuration mode
6	Informational	Access-list statement match
7	Debugging	Debugging messages

D- DHCP Event Fields Description

Field	Description
ID	A DHCP server event ID code.
Date	The date on which this entry was logged on the DHCP server.
Time	The time at which this entry was logged on the DHCP server.
Description	A description of this DHCP server event.
IP Address	The IP address of the DHCP client.
Host Name	The host name of the DHCP client.
MAC Address	The media access control (MAC) address used by the network adapter hardware of the client.

E- Firewall Event Fields Description

The format is typically as follows, however there are slight variations from version to version: Time | Action | Firewall | Interface | Product| Source | Source Port | Destination | Service | Protocol | Translation | Rule

Field Name	Description
Time	Local time on the management station
Action	accept, deny, or drop. accept=accept or pass the packet. deny=send TCP reset or ICMP port unreachable message. drop=drop packet with no error to sender
Firewall	IP address or hostname of the enforcement point
Interface	Firewall interface on which the packet was seen
Product	Firewall software running on the system that generated the message
Source	Source IP address of packet sender
Destination	Destination IP address of packet
Service	Destination port or service of packet
Protocol	Usually layer 4 protocol of packet - TCP, UDP, etc.
Translation	If address translation is taking place, this field shows the new source or destination address. This only shows if NAT is occurring.
Rule	Rule number from the GUI rule base that caught this packet, and caused the log entry. This should be the last field, regardless of presence or absence of other fields except for resource messages.

F- Application Gateway Event Fields Description

No.	Field or Activity	Description / Context / Notes
1	Requestor’s Internet Protocol (IP) address	The user’s IP address requesting information over the Internet or last connection computer (such as a proxy computer)
2	Identity and user id	The identity value and user id of the user requesting the resource at the Application Gateway.
3	Date/Timestamp	Date and time of logged activity. The time zones in one set of logs may need to be normalized with different time zones used in other logs or on a computer.
4	HTTP (Hypertext Transfer Protocol) Method	The type of method may reveal the activity. For example, the “GET” method may be used to retrieve data; the “POST” method may be used to store data, send an email, or order a product.
5	Request URI	Indicates what was requested at the server
6	HTTP Protocol Version	This is the HTTP protocol version used by the client during the request.
7	HTTP Status Code	Indicates how the server resolved the request—success, redirect, or error. For example, a 404 would indicate the requested resource was not found on this server. A 200 would indicate the request was fulfilled successfully by the Application Gateway.
8	Total bytes transferred	The size of transferred files/data (for example, image or file) not including the HTTP response headers sent by the server.
9	Referrer	Where the request originated, such as the Webpage or Uniform Resource Locator (URL) (for example, the referrer may show that the request came from Facebook)
10	User Agent String	The type of operating system, browser and other applications from the user’s computer

G – W3C Extended Log File Format

Field	Appears As	Description	Default Y/N
Date	date	The date on which the activity occurred.	Y
Time	time	The time, in coordinated universal time (UTC), at which the activity occurred.	Y
Client IP Address	c-ip	The IP address of the client that made the request.	Y
User Name	cs-username	The name of the authenticated user who accessed your server. Anonymous users are indicated by a hyphen.	Y
Service Name and Instance Number	s-sitename	The Internet service name and instance number that was running on the client.	N
Server Name	s-computername	The name of the server on which the log file entry was generated.	N
Server IP Address	s-ip	The IP address of the server on which the log file entry was generated.	Y
Server Port	s-port	The server port number that is configured for the service.	Y
Method	cs-method	The requested action, for example, a GET method.	Y
URI Stem	cs-uri-stem	The target of the action, for example, Default.htm.	Y
URI Query	cs-uri-query	The query, if any, that the client was trying to perform. A Universal Resource Identifier (URI) query is necessary only for dynamic pages.	Y
HTTP Status	sc-status	The HTTP status code.	Y
Win32 Status	sc-win32-status	The Windows status code.	N
Bytes Sent	sc-bytes	The number of bytes that the server sent.	N

Field	Appears As	Description	Default Y/N
Bytes Received	cs-bytes	The number of bytes that the server received.	N
Time Taken	time-taken	The length of time that the action took, in milliseconds.	N
Protocol Version	cs-version	The protocol version —HTTP or FTP —that the client used.	N
Host	cs-host	The host header name, if any.	N
User Agent	cs(User-Agent)	The browser type that the client used.	Y
Cookie	cs(Cookie)	The content of the cookie sent or received, if any.	N
Referrer	cs(Referrer)	The site that the user last visited. This site provided a link to the current site.	N
Protocol Substatus	sc-substatus	The substatus error code.	Y

References

Hardening Cisco Routers – O Reilly Publication

Router Security Configuration Guide – NSA

https://www.owasp.org/index.php/Logging_Cheat_Sheet

Commercial Solutions for Classified (CSfC) Virtual Private Network (VPN) Capability Package v2.0, NSA

National Information Assurance Policy v2.0

http://zeltser.com/log-management/security-incident-log-review-checklist.pdf