



Firewall Use Cases

Table of contents

Version history	2
Preface	2
Introduction and Background	3
Use Cases	3
Firewall	4
Palo Alto	4
Prerequisite	4
Enrichment	4
Log Sources	5
Normalisation	5
Alerts	6
PaloAlto URL Filtering Alerts	6
Tampering Alert	7
PaloAlto URL Filtering Alerts	7
Dashboards	8
Search Template	11
Cisco PIX ASA	12
Prerequisite	12
Enrichment	12
Log Sources	12
Normalisation	13
Alerts	13
Dashboards	18
Check Point	20
Prerequisite	20
Enrichment	20
Log Sources	20
Normalisation	21
Alerts	21
Dashboards	22
Fortinet/Fortigate NGFW	24
Prerequisite	24
Enrichment	24
Log Sources	24
Normalisation	25
Alerts	25
Dashboards	29

Version History

Version	Revision Date	Description	Implemented by
1.0	26-10-2022	Updated Firewall section - First Review	Nicolai Thomdahi & Gustav Rødsgaard

Preface

This document was created to provide better insight and basic guidelines on what to monitor with a Logpoint SIEM ingesting logs from Firewall. The document focus on the analytics part of a SIEM and thus concentrate on

- **Alerts:** Notifications that trigger based on a set of defined criteria
- **Dashboards:** Overview of multiple perspectives of the log source
- **Search Templates:** An overview of data from multiple perspectives using fields to narrow searched data/results.

The document lists the name of the Alerts, Dashboards and Search Templates that comes with Logpoint out of the box. Information on how to configure and setup of the analytics can be found in the documentation portal on docs.logpoint.com

The analytics in this document covers a subset of the analytics that exists for Active Directory and should not be seen as a complete monitoring package or compliance coverage document, but as an inspiration for basic monitoring of Active Directory to get started with.

Data collection, ingestion and storage are not covered in this document but can be found on the documentation portal docs.logpoint.com and in the installation starter pack document.

Introduction and Background

This purpose of this document is to guide the user to implement basic monitoring of specific log sources in a Logpoint SIEM platform. The document aims to make it easier for the user to get an overview of already existing alerts and dashboards in the Logpoint platform and apply them in their own environment. Furthermore, it also lists the tables and search templates that might be relevant to configure to ensure the best possible result and a better understanding of the environment as well as sorting out any unwanted results. The document is a living document that will continue to be improved over time and new use cases (areas of interest to monitor for customers/partners) will be added.

Use Cases

Use cases in this document refers to an area, domain, component of infrastructure or regulatory set of rules aligned with a framework or regulations. For each of the use cases we have selected the alerts, dashboards and search templates that are relevant to help for basic monitoring of these use cases. Alerts and dashboards are a supporting function that can help to verify controls, but they can not be seen as actual controls in a regulatory framework. A SIEM cannot stand alone against the threats and other components should be in place to increase the overall security posture of a company.

For each use case we have selected a set of alerts that are relevant for the area as well as dashboards and search templates where it creates insights and value. Be aware that these use cases are generic and for basic monitoring and might not apply to all types of environments. To the best effort the document will describe where alterations to alerts might be necessary to alerts/dashboards.

In this document you will find the use cases related to Firewalls. In case you have any requests for use cases please reach out to your local customer success responsible.

In the following sections you will find the use cases described including the technical details on what is required from a log source perspective.

Firewall

Firewall is an essential part of most organizations and enterprises today. Firewalls is primarily in charge of stopping connections from suspicious networks with next generation firewalls there is even more to log, such as Integrated intrusion prevention, Application awareness and blocking of risky apps. Hence, it is important to monitor the firewall and ingest the data into the SIEM to be able to implement Use Cases to secure your organization.

Below you will find details on how to start implementing the use case on your logpoint including the prerequisites that needs to be in place prior to setting up alerts and dashboards.

This section will include Firewalls from vendors, PaloAlto, Cisco, Fortinet, and Check Point.

Palo Alto

Palo Alto Network Firewall allows you to monitor and identify threats in your organization using Palo Alto Network Firewall data. Logpoint aggregates and normalizes logs from every Palo Alto Networks Firewall device so you can analyze the information through dashboards and security reports. Palo Alto Network Firewall dashboards provide visualization related to traffic, threat, user, content, system, and firewall configurations.

Prerequisite

The prerequisites for setting up Palo Alto Firewall Use cases revolves around configuring and propagating the Enrichment, List & Tables and Normalizations for the Log sources needed to implement the Use cases.

Enrichment

To provide the best insights for the analyst looking at logs and incidents enrichment can be applied. You can configure a custom enrichment policy with the fields you want to include from your Threat intelligence feed.

You can also use the Threat intelligence Management plugin to configure Threat Intelligence feeds such as:

- Emerging Threats
- Critical Stack
- CSIS
- MISP
- Blueliv
- Recorded Future
- STIX/TAXII
- Custom CSV

Log Sources

For the Palo Alto use case some of the PAN-os logs are needed for the alerts and dashboards to function properly. Following logs are needed from Palo Alto.

- Log type: Palo Alto PAN-OS
- Categories: Traffic logs, Threat logs, URL Filtering logs
- Log Levels: Informational, Low, Medium, High, Critical

The most common way to ingest firewall logs into logpoint is done by using the syslog collector. This document will not describe the configuration of log sources, in case you have issues configuring log sources reach out to logpoint support or your local Customer Success responsible.

Normalization

In this section it is described what kind of Normalizers you will need for normalization of the data needed for the Palo Alto Firewall use case. In below table you will find the required configurations for your normalizations policy:

Normalization Policy	
Compiled Normalizer	<ul style="list-style-type: none"> • PaloAltoCEFCcompiledNormalizer • PaloALtoNetworkFirewallCompiledNormalized
Normalizations Packages	

Alerts

The PaloAlto Alerts have two categories. First Category is URL Filtering Alerts, by using the URL Filtering capabilities of PaloAlto you can setup Alerts in logpoint to monitor for Internet usage on your clients in the organization. The Second category is for tampering and here you will find an Alert which detects Log deletion of PaloAlto logs.

PaloAlto URL Filtering Alerts

PaloAlto URL Filtering Alerts	
Technical Description	This alert is triggered whenever Domains/sites identified with scams, hacking, reserved unused domain are visited or PaloAlto identified phishing sites are visited.
Search query:	Norm_id = PaloAltoNetworkFirewall label = Traffic category in ['Grayware','Hacking','Parked','Phishing']
Considerations:	For this Alert to fire, you must configure URL filtering logging on PaloAlto PAN-OS for URL filtering Categories: Grayware, Hacking, Parked, Phishing.

PaloAlto Potential C2 Connection	
Technical Description	This alert is triggered whenever Command-and-control URLs/domains, dynamically assigned IP addresses or newly registered domain sites are visited which are oftentimes used to deliver malware payloads, for C2 traffic, malicious commands, exfiltrate data.
Search query:	norm_id = PaloAltoNetworkFirewall label = Traffic category in ['Command and Control','Dynamic DNS','Malware','Newly Registered Domain']
Considerations:	For this Alert to fire, you must configure URL filtering logging on PaloAlto PAN-OS for URL filtering Categories: Command and Control, Dynamic DNS, Malware, Newly Registered Domain

PaloAlto Illegal Content Download	
Technical Description	This alert is triggered whenever Command-and-control URLs/domains, dynamically assigned IP addresses or newly registered domain sites are visited which are oftentimes used to deliver malware payloads, for C2 traffic, malicious commands, exfiltrate data.
Search query:	Norm_id = PaloAltoNetworkFirewall label = Traffic category = 'Copyright Infringement'
Considerations:	For this Alert to fire, you must configure URL filtering logging on PaloAlto PAN-OS for Url filtering Categories: Cope

Tampering Alert

PaloAlto Log Deletion	
Technical Description	This Alert is triggered when log files are deleted by some user identified in description field
Search query:	Norm_id = PaloAltoNetworkFirewall event_category = System description = "Log*clear*"
Considerations:	For this Alert to fire, you must configure URL filtering logging on PaloAlto PAN-OS for Url filtering Categories: Cope

Dashboards

In addition to Alerts, you can configure and add PaloAlto Vendor Dashboards to add insights into your Firewall logs. The First Dashboard presented below is a more general and broader dashboard which visualize what kind of actions are being taken by your firewall. The Second dashboard General PaloAlto visualize network logs and what data-sharing platforms, or applications are being detected. The third and last dashboard is the PaloAlto Traffic dashboard. This dashboard shows network information regarding applications and bandwidth.

PaloAlto Firewall Dashboard	
Dashboard name	LP_PALOALTO: FIREWALL
Technical description	This Dashboard contains widgets regarding PaloAlto Firewall information such as: Actions, threats by location Threat data events, application firewall events, Threats on applications and Security event activity.
Widgets	<ol style="list-style-type: none"> 1. Actions – Time trend 2. Top 10 Threats by Source Location 3. Threat Data Events by User 4. Top 10 Applications by FW Events 5. Top 10 Threats by Applications 6. Top 10 Security Event Activity 7. Top 10 Firewall Rules fired and Action Taken
Considerations	Top 10 Widgets does not need to be top10 necessarily. Can be modified in the widgets underlying search.

General PaloAlto Dashboard	
Dashboard name	LP_PALOALTO: GENERAL
Technical description	This Dashboard gives generic insights into PaloAlto Firewall metric such as authenticating and traffic flow and application usage.
Widgets	<ol style="list-style-type: none"> 1. Top 10 Blocked Applications by Bandwidth 2. Top 10 Allowed Applications by Bandwidth 3. Top 10 Blocked Applications 4. Top 10 Denied Connections by Country 5. Traffic over Time 6. Heaviest Usage of Skype 7. Heaviest usage of Dropbox 8. Severity by Protocol 9. Multiple Failed Authentication from Source
Considerations	The Widgets Regarding Dropbox and Skype can be changed to any application by modifying the underlying search to match the applications name.

PaloAlto Traffic Dashboard	
Dashboard name	LP_PALOALTO: Traffic
Technical description	This Dashboard gives insight into your most common traffic by using the underlying search to present most of the data as top 10's.
Widgets	<ol style="list-style-type: none"> 1. Top 10 Source Address 2. Top 10 Destination Ports 3. Top 10 Protocols 4. Top 10 Applications by Bandwidth 5. Top 10 Destination Zones 6. Top 10 Source Zones 7. Top 10 Applications by Request 8. Traffic Through PaloAlto Network 9. Top 10 Connections 10. Bandwidth Used Per Interface 11. Top Distinct P2P Connections 12. Most Repeated Connection Profiles 13. Top 10 Session End Reasons
Considerations	Top 10 Widgets does not need to be top10 necessarily. Can be modified in the widgets underlying search.

Search Template

This Search Template Allows the Analyst to do basic Firewall Searches and filtering. The filtering options available before running the template are values such as source and destination addresses.

LP_Firewall	
Dashboard name	FIREWALL OVERVIEW
Technical description	This search template looks at Firewall Actions as a Time trend, Allowed and Denied Inbound Connections by Countries, Allowed and Denied Outbound Connections by Countries and Connection Details.
Widgets	<ol style="list-style-type: none"> 1. Firewall Action – Time trend 2. Allowed Inbound Connection by Countries 3. Denied Inbound Connections by Countries 4. Allowed Outbound Connections by Countries 5. Denied Outbound Connection by Countries 6. Connection Details

Cisco PIX ASA

The Cisco Pix/Asa network firewall enables you to monitor your network and identify threats. Logpoint can ingest, aggregate, and normalize logs from Cisco Pix/Asa Devices. Below is presentation of the Analytics premade for Cisco Pix/Asa. The Analytics can provide insight into what the Pix/Asa device is doing in your environment and dashboards visualize trends.

Prerequisite

The prerequisites for setting up CiscoPIXASA Firewall Use cases revolves around configuring and propagating the Enrichment, List & Tables and Normalizations for the Log sources needed to implement the Use cases.

Enrichment

To provide the best insights for the analyst looking at logs and incidents enrichment can be applied. You can configure a custom enrichment policy with the fields you want to include from your Threat intelligence feed. You can also use the Threat intelligence Management plugin to configure Threat Intelligence feeds such as:

- Emerging Threats
- Critical Stack
- CSIS
- MISP
- BLueliv
- Recorded Future
- STIX/TAXII
- Custom CSV

Log Sources

For the use cases you need logs from CISCO PIX ASA modules for the alerts and dashboards to function properly. Following logs are needed from CISCO.

- Log type: Syslog messages
- Log Levels: Alert Messages, Critical Messages, Error Messages, Warning Messages, Notification Messages, Informational Messages, Debugging Messages, Debugging Messages,

The most common way to ingest firewall logs into logpoint is done by using the syslog collector. This document will not describe the configuration of log sources in case you have issues configuring log sources reach out to Logpoint support or your local Customer Success responsible.

Normalization

In this section it is described what kind of Normalizers you will need for normalization of the data needed for the Cisco PIX/ASA Firewall use case. In below table you will find the required configurations for your normalizations policy:

Normalization Policy	
Compiled Normalizer	<ul style="list-style-type: none"> CiscoPIXASACompiledNormalizer
Normalizations Packages	<ul style="list-style-type: none"> LP_Cisco PIXASA LP_Cisco PIX/ASA Generic

Alerts

Below are Alerts which can found in logpoint for Cisco Pix/ASA. Alerts can aid monitoring of the firewall in your organization. It is recommended use Cisco Pix/ASA these alerts are based of the event id fields which uniquely differentiates Cisco Pix/ASA logs.

LP_CiscoPixAsa RIP Authentication Failed	
Technical Description	<p>This alert is triggered whenever ASA receives Routing Information Protocol authentication failed messages (event id 107001). This message indicates an unsuccessful attempt to attack the routing table of the ASA and should be monitored. An attacker might be trying to determine the existing keys.</p>
Search query:	<p>norm_id=CiscoPixAsaFirewall event_id=107001</p>
Considerations:	<p>If you are not familiar with the source IP address listed in this message, change your RIP authentication keys between trusted entities. An Attacker might be trying to determine the existing keys</p>

LP_CiscoPixAsa Fragment Database Limit Exceeded

Technical Description	This Alert is triggered whenever the number of matching flows cached on the ASA exceeds the limit configured by the user using the “access-list-deny-flow-max” command
Search query:	norm_id=CiscoPixAsaFirewall event_id=106101
Considerations:	Use the Access-list-deny-flow-max command to set a max in which you minimize false positives and still are able to catch a possible DoS attack.

LP_CiscoPixAsa Deny Flow Limit Reached

Technical Description	This alert is triggered whenever an user has exceeded the user authentication proxy limit, and has opened too many connections to the proxy (event id 109017)
Search query:	norm_id=CiscoPixAsaFirewall event_id=109017
Considerations:	This might indicate a DoS attack. If this alert is firing on regular user activity, it is recommended to increase the proxy limit.

LP_CiscoPixAsa Decapsulated IPsec Packet with IP Fragment with small Offset

Technical Description	This Alert is Triggered whenever Decapsulated IPsec packet with IP fragment with small offset is found (event id 402118)
Search query:	norm_id=CiscoPixAsaFirewall event_id=402118
Considerations:	A decapsulated IPsec packet included an IP fragment with an offset less than or equal to 128bytes. The latest version of the security architecture for IP RFC recommends 128 bytes as the minimum IPfragment offset to prevent reassembly attacks. This may be part of an attack. This message is rate limited to no more than one message every five seconds.

LP_CiscoPixAsa DoS Attack

Technical Description	This alert is triggered whenever adversary attempt to perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users.
Search query:	norm_id=CiscoPixAsaFirewall label=Dos label=Attack source_address=*
Considerations:	This alert might produce multiple unsuccessful Dos attack attempts and it is worth considering narrowing the alerting down to e.g. seeing multiple attacks from same IP or multiple attacks over a certain period of time. If the cause is an attack, you can deny the host by using ACLs

LP_CiscoPixAsa ICMP Message not Related to any session

Technical Description	This Alert is Triggered whenever the ICMP message is not related to any session (event id 313005)
Search query:	norm_id=CiscoPixAsaFirewall event_id = 313005
Considerations:	If the cause is an attack, you can deny the host by using ACLs.

LP_CiscoPixAsa Mac Spoofing or Misconfiguration

Technical Description	This alert is triggered whenever packet from the offending MAC address on the specified interface, but the source MAC address in the packet is statically bound to another interface in the configuration (event id 322001)
Search query:	norm_id=CiscoPixAsaFirewall event_id= 322001
Considerations:	Check the configuration on the device to figure out whether this is a misconfiguration or a potential mac spoofing event.

LP_CiscoPixAsa Malicious pattern in email

Technical Description	Event 108003 is generated when the ASA detects a malicious pattern in an email address and has hence dropped the connection.
Search query:	norm_id=CiscoPixAsaFirewall event_id= 108003
Considerations:	As the connection is already dropped it could be worth investigating if the email was malicious to monitor the accuracy of this alert

LP_CiscoPixAsa Man in the Middle Attack

Technical Description	This alert is triggered whenever the peer certificate includes a subject name that does not match the output of the "ca verifycertdn" command, indication of the man in the middle(event_id=320001)
Search query:	norm_id=CiscoPixAsaFirewall event_id= 320001
Considerations:	This Alert does not need any action as such. However, activating the alert can give insights into the Network.

LP_CiscoPixAsa Per Client Embryonic Connection limit was exceeded

Technical Description	This alert is triggered whenever per client embryonic connection [connection which is in the process of being established] limit is exceeded (event id 201012).
Search query:	norm_id=CiscoPixAsaFirewall event_id= 201012
Considerations:	When the limit is reached any new connection request will be proxied by the Secure Firewall ASA to prevent a SYN flood attack. It is possible to increase the amount of allowed embryonic connections

LP_CiscoPixAsa Remote Access Denied

Technical Description	This alert is triggered whenever remote connection is denied.
Search query:	norm_id=CiscoPixAsaFirewall label=Remote label=Connection label=Deny
Considerations:	This alert can give insight into how

LP_CiscoPixAsa Rip Packet Failed	
Technical Description	This alert is triggered whenever the rip packet fails and may be an attempt to exploit the routing table of the ASA (event id 107002).
Search query:	norm_id=CiscoPixAsaFirewall event_id=107002
Considerations:	This message indicates a possible attack and should be monitored. The packet has passed authentication, if enabled, and bad data is in the packet. Monitor the situation and change the keys if there are any doubts about the originator of the packet.

LP_CiscoPixAsa Suspicious network activity	
Technical Description	This alert is triggered whenever the rip packet fails and may be an attempt to exploit the routing table of the ASA (event id 107002).
Search query:	norm_id=CiscoPixAsaFirewall label=Connection label=Deny chart count() as Event by source_address search Event > 10
Considerations:	You might want to consider how many Events you want to have logged before triggering the Alert. The Default is 10.

Dashboards

The Cisco Pix/Asa enables you to see trends and status of the Device. You can with this dashboard gather information regarding network, CPU remote logins and more. It is always recommended to further tune your dashboard to fit your need organization's needs.

Cisco: Pix ASA-Overview Dashboard	
User Management Dashboard	LP_CISCO: PIX ASA -OVERVIEW
Technical description:	This Dashboard contains 23 widgets detailing information from Cisco PIX ASA firewall logs. Most of the data is presented in top 10s.
Widgets	<ol style="list-style-type: none"> 1. Top 10 Successful User Authentication 2. Top 10 Failed User Authentication 3. Top 10 Blocked Ports 4. Dropped Packets timeline 5. Accepted Packet timeline 6. Top 10 protocols by Action 7. Top 10 outgoing sources 8. Top 10 incoming sources 9. Top 10 Dropped Packet source 10. Top 10 Successful Remote User Login 11. Top 10 Failed Remote Login 12. Top 10 Successful Network Login 13. Top 10 Failed Network Login 14. Interface Status 15. CPU Usage timeline 16. Number of connections 17. Top 10 ports in inbound connections 18. Top 10 ports in outbound connections 19. Top 10 outbound destinations by Geolocation 20. Top 10 inbound sources by Geolocation 21. Top 10 Data Transfer 22. Top 10 outbound data transfer 23. Top 10 inbound received data size
Considerations:	<p>Top 10 Widgets does not need to be top10 necessarily.</p> <p>Can be modified in the widgets underlying search.</p>

Check Point

The Check Point R81 manages network security solutions in your environment. These solutions can be forwarded to logpoint and have further analytics applied to them. This can give insights into threat prevention and network infrastructure.

Prerequisite

Enrichment

You can also use the Threat intelligence Management plugin to configure Threat Intelligence feeds such as:

- Emerging Threats
- Critical Stack
- CSIS
- MISP
- BLueliv
- Recorded Future
- STIX/TAXII
- Custom CSV

Log Sources

For the use cases you need logs from Check Point Firewall modules for the alerts and dashboards to function properly. Following logs are needed from Check Point firewalls.

- Log type: Syslog messages
- Log Levels: Alert Messages, Critical Messages, Error Messages, Warning Messages, Notification Messages, Informational Messages, Debugging Messages, Debugging Messages,

The most common way to ingest firewall logs into logpoint is done by using the syslog collector. This document will not describe the configuration of log sources in case you have issues configuring log sources reach out to logpoint support or your local Customer Success responsible.

Normalization

Normalization Policy	
Compiled Normalizer	<ul style="list-style-type: none"> • Check PointFirewallCEFCompiledNormalizer • Check PointOPsecCompiledNormalizer • Check PointInfinityCompiledNormalizer
Normalizations Packages	<ul style="list-style-type: none"> • LP_Check Point Firewall • LP_Check Point Firewall Opsec Generic • LP_Check Point Firewall Process • LP_Check Point Endpoint Security

Alerts

LP_Check Point IP Port Change	
Technical Description	This alert is triggered whenever the IP port is changed.
Search query:	norm_id="Check Point*Firewall*" label=IP label=Port label=Change
Considerations:	

LP_Check Point Secure Remote Login	
Technical Description	This alert is triggered whenever a user logs in secure remote login.
Search query:	norm_id="Check Point*Firewall*" label=Login label=Remote
Considerations:	

Dashboards

Check Point Opsec Firewall Dashboard	
Dashboard name	LP_Check Point Firewall Opsec
Technical description	This Dashboard contains widgets detailing information from Check Point firewall logs. Most of the data is presented in top 10s.
Widgets	<ol style="list-style-type: none"> 1. Check Point Actions 2. Top 10 Denied inbound Connections 3. Top 10 Allowed inbound Connection by Countries 4. Top 10 Allowed Outbound Connection by Countries 5. Top 10 Destination Countries by Service 6. Top 10 Protocols 7. Top 10 Denied Ports 8. Top 10 Services 9. Top 10 Firewall Rules Hit 10. Top 10 Denied Outbound Connection by Countries 11. Denied Connections – list
Considerations	Top 10 Widgets does not need to be top10 necessarily. They can be modified in the widgets underlying search.

Check Point Firewall Dashboard	
Dashboard name	LP_Check Point Firewall
Technical description	This Dashboard contains widgets detailing information from Check Point firewall logs. Most of the data is presented in top 10s.
Widgets	<ol style="list-style-type: none"> 1. Log Count by Severity – Time trend 2. Log Count – Time trend 3. Top 10 Allowed Source Addresses 4. Top 10 Allowed Destination Addresses 5. Top 10 Denied Source Addresses 6. Top 10 Denied Destination Addresses 7. Allowed/Denied Connections by IP 8. Top 10 Dropped Connections 9. Top 10 Decrypted Connections 10. Top 10 Encrypted Connections 11. Secure Remote Login 12. IP-Port Changed – List 13. Top Actions 14. Top Protocols
Considerations	Top 10 Widgets does not need to be top10 necessarily. They can be modified in the widgets underlying search.

Fortinet / Fortigate NGFW

Fortinet Firewalls enables you with several critical security features such as stateful inspection, antivirus, Intrusion prevention and Virtual Private Networks. Logpoint aggregates and normalizes logs from Fortinet firewall devices so you can analyze logs through dashboards and Alerts. The Fortinet dashboards allows you to investigate Fortinet Attack logs, Traffic logs and Web logs.

Prerequisite

Enrichment

You can also use the Threat intelligence Management plugin to configure Threat Intelligence feeds such as:

- Emerging Threats
- Critical Stack
- CSIS
- MISP
- BLueliv
- Recorded Future
- STIX/TAXII
- Custom CSV

Log Sources

For the Fortinet Use cases presented here. It is necessary to have FortiGate Next Generation Firewall sending logs to your logpoint instance.

- Log type: Syslog messages
- Log Levels: 0 (Emergency), 1 (Alert), 2 (Critical), 3 (Error), 4 (Warning), 5 (Notification), 6 (Information), 7 (Debug)

The most common way to ingest firewall logs into logpoint is done by using the syslog collector. This document will not describe the configuration of log sources, in case you have issues configuring log sources reach out to Logpoint support or your local Customer Success responsible.

Normalization

Normalization Policy	
Compiled Normalizer	<ul style="list-style-type: none"> • FortiCEFCompiledNormalizer • FortiOSCompiledNormalizer
Normalizations Packages	<ul style="list-style-type: none"> • LP_FortiAnalyzer • LP_FortinetConnect • LP_Forti Authenticator v4

Alerts

Fortigate Alerts can aid your security team to automate certain tasks. The Fortigate Alerts are based off the actions performed by the Fortigate device. This includes Actions based on Network Activity, and Fortigate User management.

LP_Fortigate Admin Login Disable	
Technical Description	This Alert is triggered whenever administrator login is disabled in the system
Search query:	Norm_id=Forti* event_category=event sub_category=System message_id=32021 user=*
Considerations:	

LP_FortiGate Anomaly	
Technical Description	This alert is triggered whenever there is any anomaly in the system.
Search query:	norm_id=Forti* event_category=anomaly sub_category=anomaly log_level=alert attack=* process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	

LP_FortiGate Antivirus Botnet Warning

Technical Description	This alert is triggered whenever there is any botnet warning from Antivirus
Search query:	norm_id=Forti* (event_category=av OR event_category=antivirus) sub_category=botnet message_id=9248 process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	

LP_FortiGate Antivirus Scan Engine Load Failed

Technical Description	This alert is triggered whenever there is Antivirus Scan engine Load Failure
Search query:	norm_id=Forti* event_category=av sub_category=scanerror message_id=8974 process geoip(source_address) as source_location process geoip(destination_address) as destination_location
Considerations:	

LP_FortiGate Attack

Technical Description	This Alert is triggered whenever there's any type of attack in the system
Search query:	norm_id=Forti* attack=* process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	

LP_Critical Events	
Technical Description	This alert is triggered whenever there is any critical events in the system.
Search query:	norm_id=Forti* event_category=event sub_category=system log_level=critical
Considerations:	

LP_FortiGate IPS Events	
Technical Description	This Alert is triggered whenever there is any intrusion attempts in the system.
Search query:	norm_id=Forti* event_category=utm sub_category=ips user=* process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	

LP_FortiGate Malicious URL Attack	
Technical Description	This alert is triggered when there is any malicious attack in the system.
Search query:	norm_id=Forti* event_category=ips sub_category="malicious-url" message_id=16399 process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	This Alert rule is valid only for FORTiOS V6.0.4

LP_FortiGate VPN SSL User Login Failed

Technical Description	This alert is triggered whenever there is VPN SSL login failure of a user.
Search query:	norm_id=Forti* event_category=event sub_category=vpn message_id=39426 user=*
Considerations:	

LP_FortiGate Virus

Technical Description	This alert is triggered whenever there is any Virus attack.
Search query:	norm_id=Forti* event_category=utm sub_category=virus process geoip(source_address) as source_country process geoip(destination_address) as destination_country
Considerations:	

LP_Fortigate TCP-UDP Anomaly

Technical Description	This alert is triggered whenever there is any TCP/UDP Anomaly in the system
Search query:	norm_id=Forti* event_category=anomaly sub_category=anomaly message_id=18432 process geoip(source_address) as source_location process geoip(destination_address) as destination_location
Considerations:	

Dashboards

The FortiGate Dashboards enables you to quickly identify trends and health in your environment. The Dashboards are separated by categories. There is a General FortiGate dashboard, Traffic dashboard, Web Dashboard and lastly an Attack Dashboard.

FortiGate General Dashboard	
Dashboard name	LP_FORTIGATE: GENERAL
Technical description	This Dashboard contains widgets detailing information from FortiGate firewall logs. Most of the data is presented in top 10s.
Widgets	<ol style="list-style-type: none"> 1. Top Severity by Timetrend 2. Top 10 Sub Categories 3. Top 10 Destination Addresses 4. Top 10 Source Addresses 5. Top 10 Applications Usages 6. Top 10 Source Ports 7. Top 10 Desetination Ports 8. Top 10 Secure Locations 9. Top 10 Destination Locations 10. Top 10 Services Usages 11. Events Descriptions 12. Top Actions over Applications 13. Top 10 Destination Locations by Sessions 14. Top 10 Source Location by Sessions 15. Configuration Changes - Details
Considerations	Top 10 Widgets does not need to be top10 necessarily. Can be modified in the widgets underlying search.

Fortigate Traffic	
Dashboard name	LP_FORTIGate: TRAFFIC
Technical description	This Dashboard contains widgets detailing information from FortiGate firewall logs. Most of the data is presented in top 10s.
Widgets	<ol style="list-style-type: none"> 1. Forward Traffic Over Time 2. Bandwidth Usage for Past 24 Hours 3. Bandwidth Usage by Source Locations 4. Bandwidth Usage by Destination Location 5. Top 10 Source Addresses by Bandwidth Usage 6. Top 10 Destination Addresses by Bandwidth Usage 7. Top 10 Applications by Bandwidth Usage 8. Bandwidth Used by Source Interfaces 9. Bandwidth Usage by Destination interface 10. Top 10 Source Address with High Outbound Traffic 11. Top 10 Destination Address with high Outbound Traffic 12. Top 10 Source Address in Denied Connection 13. Top 10 Destination Address in Denied Connection 14. Denied Connection Details
Considerations	

Fortgite Attack Dashboard	
Dashboard name	LP_FORTIGate: ATTACK
Technical description	This Dashboard contains widgets detailing information from FortiGate firewall logs. Most focused on different types of attacks.
Widgets	<ol style="list-style-type: none"> 1. Attacks – List 2. Distinct Count of Attacks by Critical Level 3. Distinct Count of Incomming or Outgoing Attacks 4. Top Actions on Distinct Attacks 5. Top Distinct Attacks by Source Locations 6. Top Distinct Attacks by Destination Locations 7. Top Distinct Attacks on Source Ports 8. Top Distinct Attacks on Destination Ports 9. Attack – Details
Considerations	Even though the dashboard lists “attacks” it might not be actual attacks but could be indicators of an attack and some might be false positives.

Fortgite Attack Dashboard	
Dashboard name	LP_FORTIGATE: WEB
Technical description	This Dashboard contains widgets detailing information from FortiGate Web logs.
Widgets	<ol style="list-style-type: none"> 1. Action Host – List 2. Bandwidth Received or Sent by Host Details 3. Top 10 Web Application Sub-Categories 4. Web request Blocked Details – List 5. Web Request Details – List 6. Web Request – Timechart for Past Hour
Considerations	Web logs need to part of the solution before this dashboard provides any results.