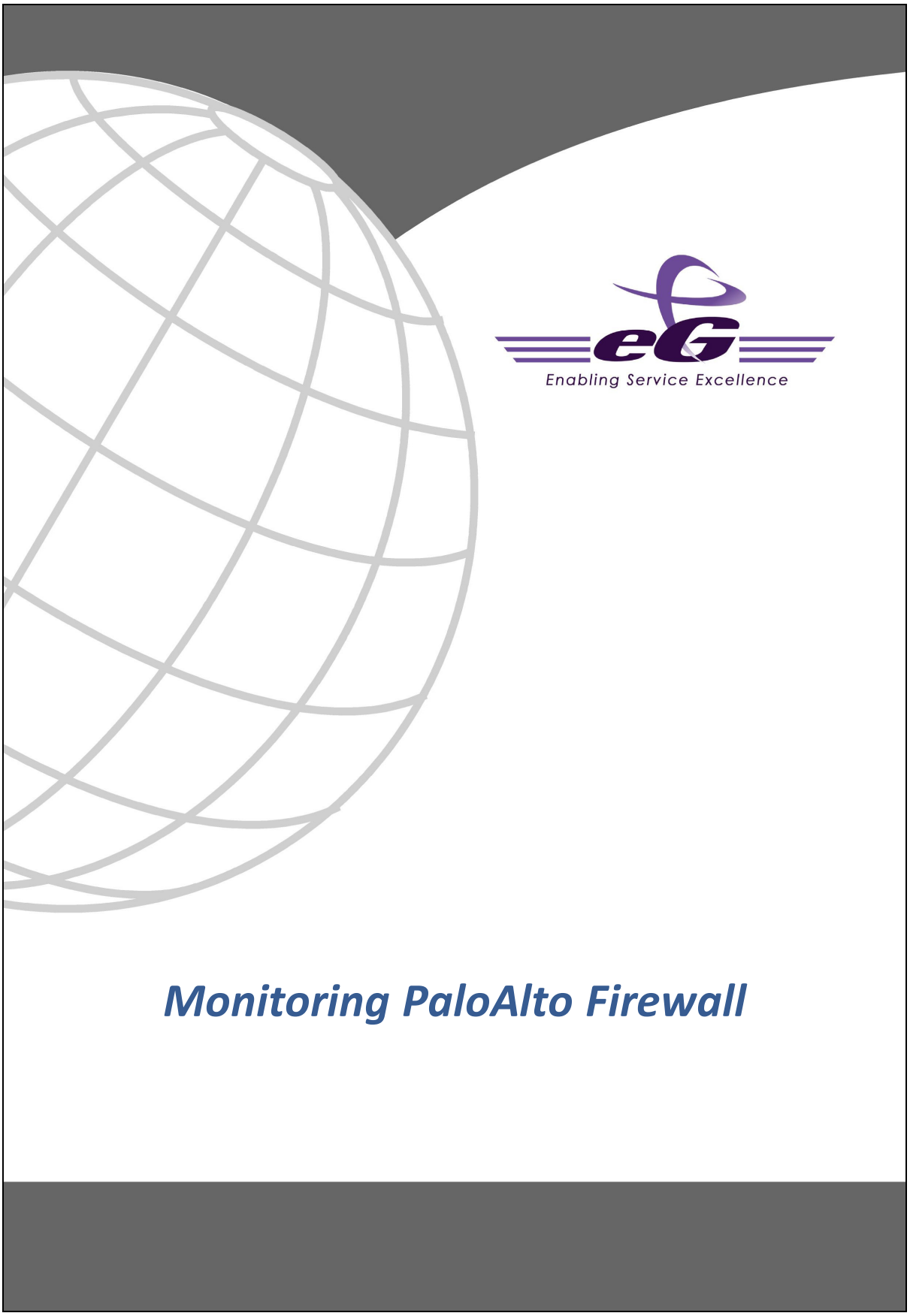


Monitoring PaloAlto Firewall

Table of contents

Table of Figures

1

Monitoring the PaloAlto Firewall

The Palo Alto firewall - a next generation firewall prevents threats, and safely enables applications, across a versatile set of high-performance use cases (e.g., Internet Gateway, DC, and SP environments). This firewall is based on a consistent *Single Pass architecture* which when implemented on both physical and virtual appliances is designed to secure these appliances from malicious threats and attacks. The Palo Alto firewall attempts to fully classify the traffic passing through the firewall i.e., this single pass architecture allows for precise and flexible control of traffic based on: applications, users and the information content of the traffic i.e., sensitive data patterns and a variety of other context. The single pass architecture's *scan it all scan it once* approach enables high security to the organization.

Uninterrupted firewall operations are imperative to keep hackers and harmful viruses at bay. Any issue in the configuration, state, or resource usage of the firewall can bring its operations to a halt, leaving your network and all mission-critical applications operating within defenceless against malicious viruses and unscrupulous users! It is hence important that the performance of the firewall is monitored 24x7.

eG Enterprise provides a specialized Palo Alto Firewall monitoring model (see Figure 1.1), which periodically polls the SNMP MIB of the firewall to measure the high availability status, session utilization, gateway utilization, and the tunnels that were created on the firewall, and notifies administrators of potential threats or configuration issues with the firewall.

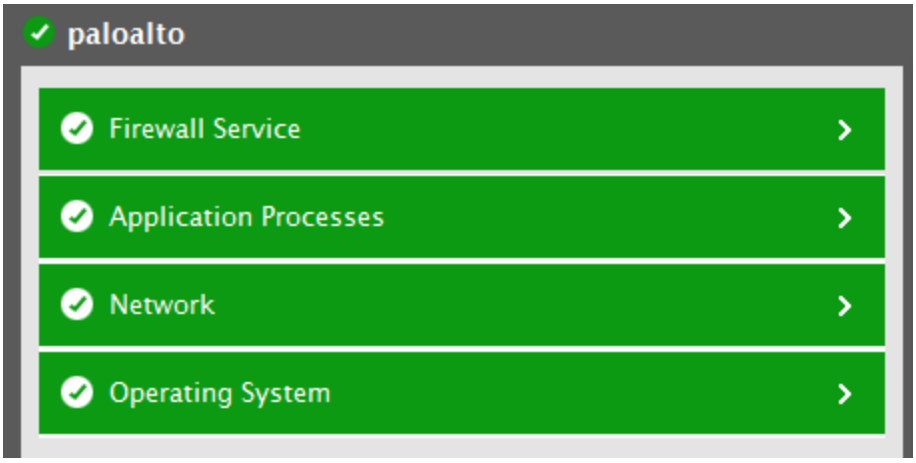


Figure 1.1: The layer model of the Palo Alto firewall

Using the metrics reported , administrators can find quick and accurate answers to the following performance issues:

- Is the firewall available over the network? How is the network connectivity to the firewall – solid or flaky?
- Is the high availability of the firewall enabled or disabled? If enabled, what is the mode of high availability configuration?

- How many sessions are currently active on the firewall? Which type of sessions are causing network overload - is it TCP? UDP? SSL Proxy?
- How many tunnels are active on a GlobalProtect subscription? How well the GlobalProtect gateways are utilized?
- How many sessions are active on each virtual system of the firewall? What is the session utilization on each virtual system?

The *Operating System*, *Network* and *Application Processes* layers of the Palo Alto Firewall model is similar to that of a Windows server model. Since these tests have been dealt with in the *Monitoring Unix and Windows Servers* document, Section **1.1** focuses on the *Firewall Service* layer.

1.1 The Firewall Service layer

This layer tracks the high availability status of the firewall and the mode using which the high availability setup is configured, the active sessions count, the active sessions count and session utilization on each virtual system, number of tunnels when the GlobalProtect subscription is available, GlobalProtect gateway utilization etc.

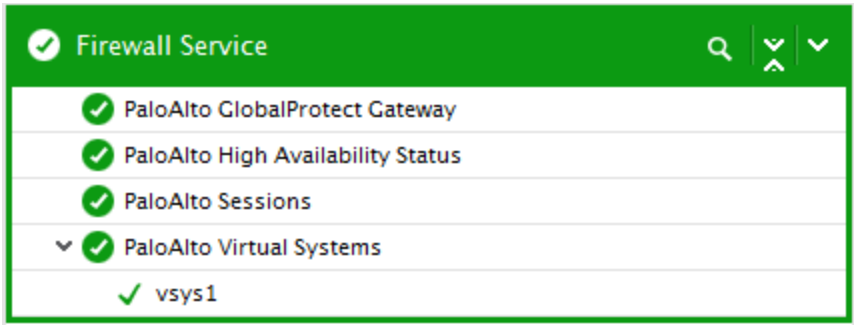


Figure 1.2: The Firewall Service layer

1.1.1 PaloAlto High Availability Status Test

High availability (HA) is a configuration in which two firewalls are placed in a group and their configuration is synchronized to prevent a single point of failure on your network. A heartbeat connection between the firewall peers ensures seamless failover in the event that a peer goes down. Setting up two firewalls in an HA pair provides redundancy and allows you to ensure business continuity.

The Palo Alto firewalls can be deployed as high availability (HA) pair with session and configuration synchronization to provide uninterrupted operation in any session. The high availability configuration always ensures that one of the two firewalls is available for maintaining the network traffic so that the downtime of the network is reduced considerably. The firewalls can be configured as stateful Active/Passive or Active/Active high availability pair.

If the high availability of the firewall is challenged, then the your environment may be rendered defenceless against unsavory virus attacks and unauthorized access, both of which can cause irreparable damage. Hence, to make sure that your environment stays protected 24X7x365 from network threats, it is necessary to

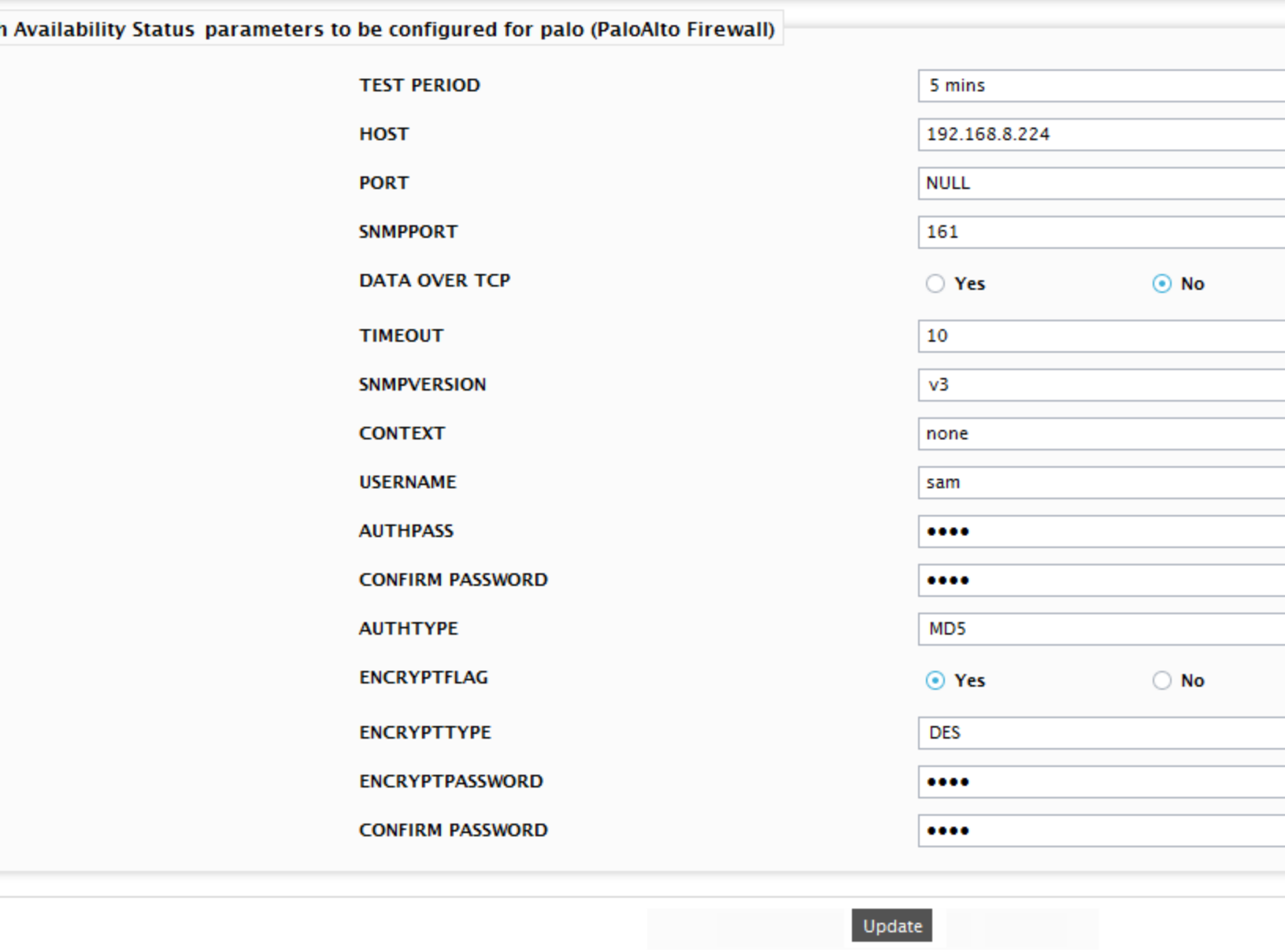
monitor the high availability status of the Palo Alto Firewall. The **PaloAlto High Availability Status** test exactly helps you in this regard.

By continuously monitoring the Palo Alto Firewall, this test reveals the high availability status of the firewall and the mode in which the firewall is configured for high availability.

Target of the test : A Palo Alto Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the firewall being monitored



Configurable parameters for the tests

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Palo Alto Firewall
3. **SNMPPORT** – The port at which the Palo Alto Firewall exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **V3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall.

This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when v3 is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG**– This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some

environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the target firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>High availability status:</td><td>Indicates the high availability status of the firewall.</td><td></td><td>The numeric values that correspond to these states are as follows:
<table><tr><th>State</th><th>Numeric Value</th></tr><tr><td>Disabled</td><td>0</td></tr><tr><td>Enabled</td><td>100</td></tr></table>
Note:
By default, this measure reports the above- mentioned State s to indicate whether/not the high availability is enabled for the PaloAlto firewall . However, in the graph of this measure, the same will be represented using the numeric equivalents – 0 and 100 only.</td></tr>
<tr><td>High availability mode:</td><td>Indicates the mode in which the firewall is configured for high availability.</td><td></td><td>The numeric values that correspond to these modes are as follows:
<table><tr><th>Mode</th><th>Numeric Value</th></tr><tr><td>Disabled</td><td>0</td></tr><tr><td>Active-Passive</td><td>1</td></tr><tr><td>Active-Active</td><td>2</td></tr></table>
Note:
By default, this measure reports the above-mentioned Modes to indicate in which mode the firewall is configured for high availability. However, in the graph of this measure, the same will be represented using the numeric equivalents – 0 and 2 only.</td></tr>
</table>

1.1.2 PaloAlto Sessions Test

The Palo Alto firewall lets users to create sessions using different protocols such as Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Internet Control Message Protocol (ICMP) or SSL Proxy connection. These communication protocols ensure reliability, end-to-end delivery and flow and error control of data during the user sessions.

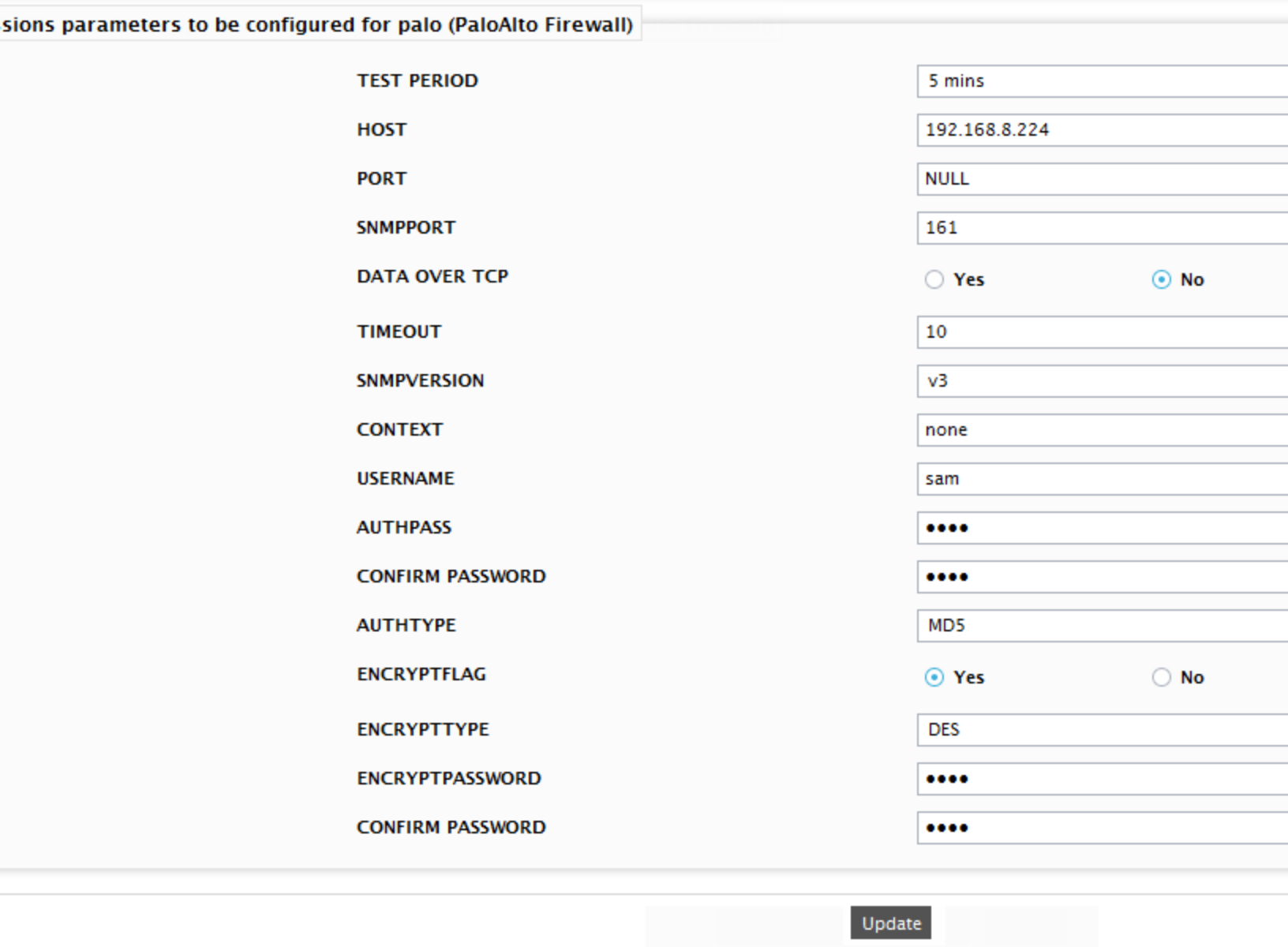
Frequent overload condition on a firewall can actually cause irreversible damage to the firewall. If the Palo Alto Firewall is overloaded with sessions, it may actually slow down the request processing capability of the firewall. Under such circumstances, administrators will have to identify the type of sessions that are causing the overload – are they TCP sessions? UDP sessions? ICMP sessions? SSL Proxy sessions? – and investigate why the count of such sessions are unusually high on the firewall. Moreover it is the onus of the administrators to keep track of the session utilization as well. If the session utilization is high throughout, it may result in overload condition with the sessions hogging excessive network bandwidth. This may in turn cause slowdown of the firewall which when left unattended will lead to performance degradation. Administrators should therefore constantly monitor the sessions of the firewall and figure out what type of sessions are frequently causing overload. The **PaloAlto Sessions** test helps administrators in this regard.

This test monitors the sessions on the Palo Alto Firewall and reports the number of active TCP, UDP, ICMP and SSL Proxy sessions. In addition, this test reveals the overall session utilization and the SSL Proxy session utilization. This way, administrators can keep track of sudden spikes in the number of sessions and proactively be alerted to overload condition, if any.

Target of the test : A Palo Alto Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the firewall being monitored



Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed.
2. **HOST** – The IP address of the Palo Alto Firewall.
3. **SNMPPORT** – The port at which the PaloAlto firewall exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **V3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall.

This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when v3 is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when v3 is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG**is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some

environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the target firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active sessions:	Indicates the total number of sessions that are currently active on the firewall.	Number	This measure is a good indicators of session load on the firewall.
Active UDP sessions:	Indicates the number of UDP sessions that are currently active on the firewall.	Number	A high value of this measure could indicate a UDP session overload on the firewall.
Active TCP sessions:	Indicates the number of TCP sessions that are currently active on the firewall.	Number	A high value of this measure could indicate a TCP session overload on the firewall.
Active ICMP sessions:	Indicates the number of ICMP sessions that are currently active on the firewall.	Number	A high value of this measure could indicate an ICMP session overload on the firewall.
Active SSL Proxy sessions:	Indicates the number of SSL Proxy sessions that are currently active on the firewall.	Number	A high value of this measure could indicate SSL Proxy session overload on the firewall.
Session utilization:	Indicates the utilization percentage of the sessions on the firewall.	Percentage	A high value for this measure indicates an overload condition on the firewall.
SSL Proxy session utilization:	Indicates the utilization percentage of SSL Proxy sessions on the firewall.	Percentage	A high value for this measure could indicate an overload of the SSL Proxy sessions on the firewall.

1.1.3 PaloAlto Virtual Systems Test

Virtual systems are multiple, logical firewall instances within a single Palo Alto Networks physical firewall. Each virtual system is an independent, separately managed logical firewall with its traffic kept separate from that of others. A typical scenario where virtual systems are used is a deployment scenario i.e., two physical firewalls (a HA pair) can be configured as virtual systems for use by tenants of a Managed Security Service Provider. In such environments, administrators can exists in different levels of the system. With the help of virtual systems, administrators can control access to the device level as well as specific management functions (enable, disable, hide) for each firewall customer or user. The flexibility and efficiencies of virtual systems present managed service providers (MSP) and enterprises with some very attractive possibilities to enhance business efficiencies such as improved scalability, low capital expenditure and reduced operational cost.

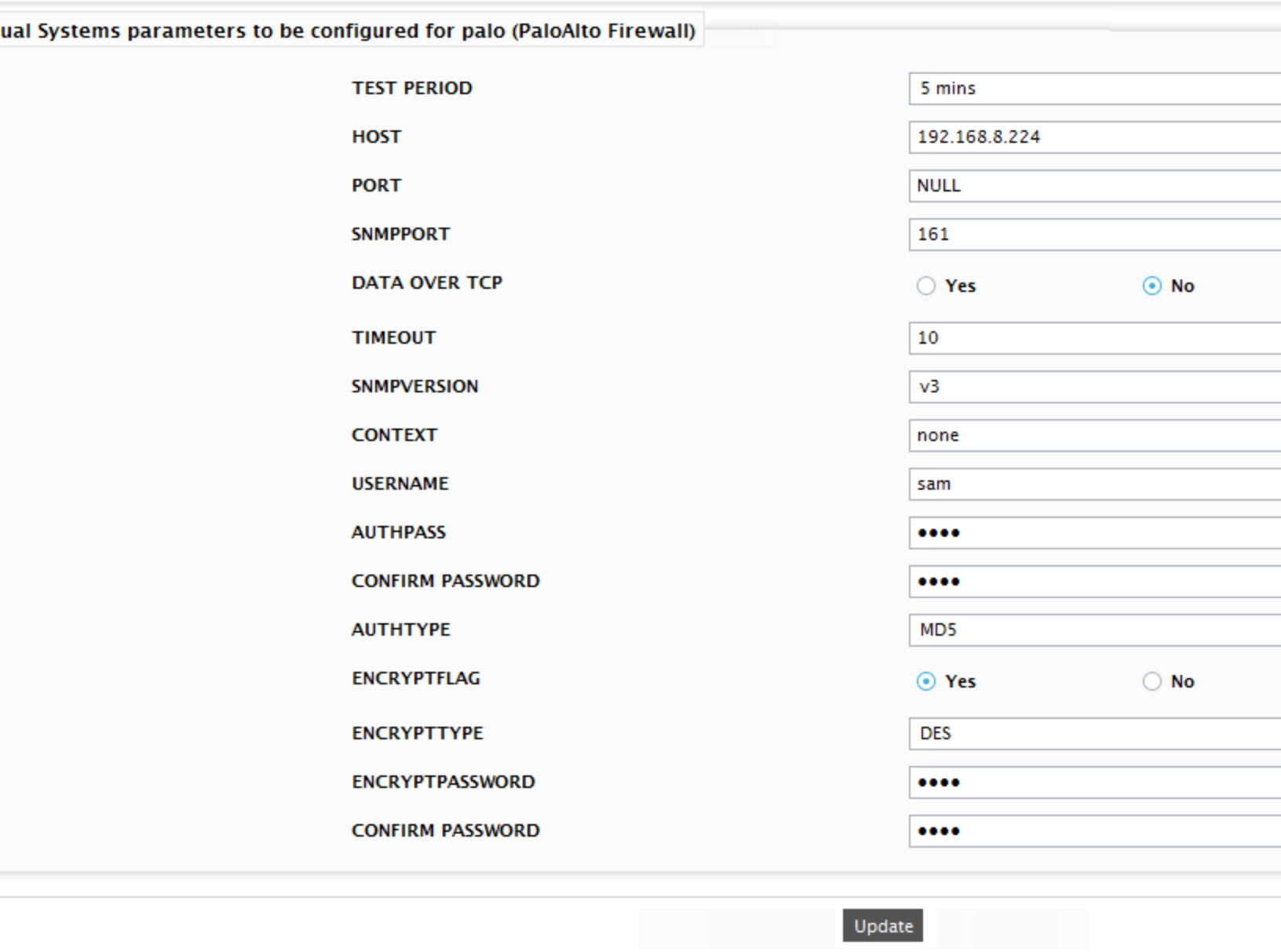
For efficiently monitoring the traffic through the physical firewall, each administrator of the environment can be assigned with a limited number of virtual systems. If the super administrator of the environment wants to figure out how well sessions are utilized in a virtual server, then he/she can monitor the individual virtual systems and figure out the session load on each virtual system. By continuously monitoring the virtual systems, the super administrator can easily identify the virtual system that is overloaded and further investigate the real reason behind such overload. The **PaloAlto Virtual Systems** test helps administrators to continuously monitor the session load on the virtual systems.

For each virtual system configured on the Palo Alto Firewall, this test reports the number of active sessions that are active on the virtual system and the percentage of sessions utilized. This test provides administrators effective pointers on the current session load on the virtual systems and identify overloaded virtual systems, if any.

Target of the test : A Palo Alto Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for each virtual system configured on the target firewall being monitored



Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Palo Alto Firewall
3. **SNMPPORT** – The port at which the Palo Alto Firewall exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **V3**, then select the corresponding option from this list.
5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall.

This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.

6. **USERNAME** – This parameter appears only when v3 is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when v3 is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.
16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some

environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the target firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Active sessions:	Indicates the number of sessions that are active on this virtual system.	Number	This measure is a good indicator of the session load on the virtual system. Compare the value of this measure across virtual systems to identify the virtual system that is constantly overloaded.
Session utilization:	Indicates the percentage of utilization of session on this virtual system.	Percentage	A high value for this measure is an indication of overload condition on the virtual system.

1.1.4 PaloAlto GlobalProtect Gateway Test

The security subscriptions on the Palo Alto Firewall allows you to safely enable applications, users and content by adding natively integrated protection from known and unknown threats both on and off the network. These security subscriptions are purpose-built to share context and prevent threats at every stage of an attack, allowing you to enable singular policies and automated protection that secure your network and remote workforce while simplifying management and enabling your business. Some of these subscriptions are:

- AutoFocus
- GlobalProtect
- URL Filtering PAN-DB
- Threat Prevention and
- WildFire

In a corporate environment, most of the employees prefer to work outside of their corporate boundaries due to various reasons like travel, work from home facility etc. Though this increased workforce mobility would increase the productivity of the employees along with flexibility, it also simultaneously introduces significant security threats to the corporate environment. The GlobalProtect provides a complete infrastructure for managing the mobile workforce of a corporate by enabling secure access to all the users, regardless of what

devices they are using or where they are located. The GlobalProtect infrastructure comprises of the following components:

- GlobalProtect Portal
- GlobalProtect gateways
- GlobalProtect Client and
- GlobalProtect Mobile Security

Every client system that participates in the GlobalProtect network receives configuration information from the portal, including information about available gateways as well as any client certificates that may be required to connect to the GlobalProtect gateway(s) and/or the Mobile Security Manager. In addition, the portal controls the behavior and distribution of the GlobalProtect agent software to both Mac and Windows laptops. (On mobile devices, the GlobalProtect app is distributed through the Apple App Store for iOS devices or through Google Play for Android devices). If you are using the Host Information Profile (HIP) feature, the portal also defines what information to collect from the host, including any custom information you require. The two types of configuring the GlobalProtect gateway are:

- **External gateways** - Provide security enforcement and/or virtual private network (VPN) access for your remote users. VPN access is provided through an IPSec or SSL tunnel between the client and a tunnel interface on the gateway firewall.
- **Internal gateways** - An interface on the internal network configured as a GlobalProtect gateway for applying security policy for access to internal resources. When used in conjunction with User-ID and/or HIP checks, an internal gateway can be used to provide a secure, accurate method of identifying and controlling traffic by user and/or device state. Internal gateways are useful in sensitive environments where authenticated access to critical resources is required. You can configure an internal gateway in either tunnel mode or non-tunnel mode.

Whenever an infrastructure is accessed from an external network, administrators should keep constant vigil on the traffic flowing through the established tunnels. The same logic applies to the tunnels that were created to access an infrastructure that is guarded using the Palo Alto Firewall with the GlobalProtect subscription. If the number of tunnels suddenly increases or if the GloblaProtect gateway is utilized to the maximum frequently, then the firewall may not function efficiently resulting in a few tunnels hogging the bandwidth resources and choking the network! To avoid this, administrators should periodically check the number of tunnels and the utilization of the GlobalProtect gateways. This is where the **PaloAlto GlobalProtect Gateway Utilizations** test helps!

This test continuously monitors the GlobalProtect subscription enabled Palo Alto Firewall and reports the number of tunnels created on the firewall using the GlobalProtect subscription and the utilization of the GlobalProtect gateways. Using this test, administrators can easily identify malicious threats to their network if the number of tunnels are abnormally high and fine-tune the number of GlobalProtect gateways if the gateway utilization is high throughout.

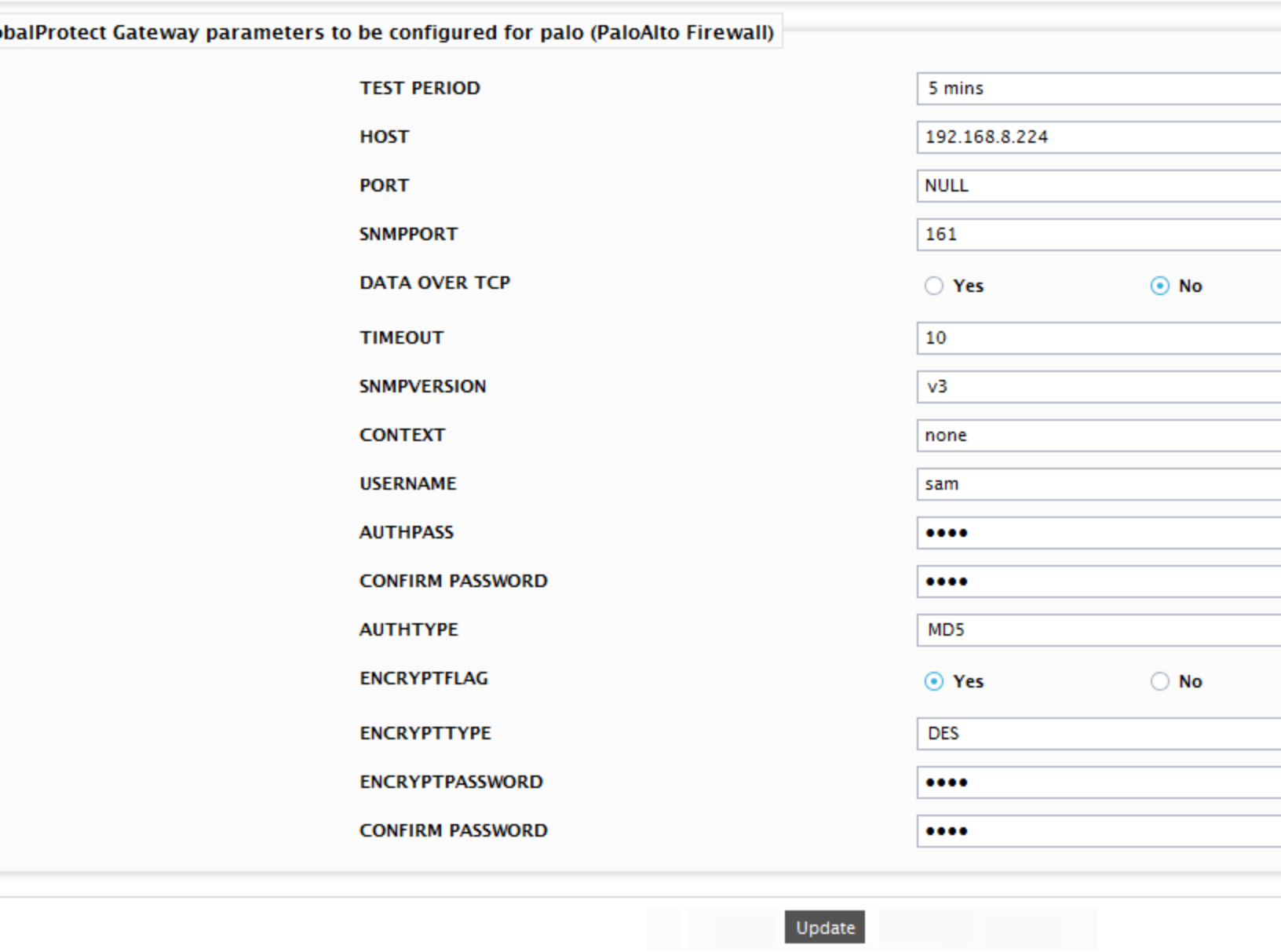
Note:

This test will report metrics only if you have subscribed to GlobalProtect.

Target of the test : A Palo Alto Firewall

Agent deploying the test : An external agent

Outputs of the test : One set of results for the firewall being monitored.



Configurable parameters for the test

1. **TEST PERIOD** - How often should the test be executed
2. **HOST** – The IP address of the Palo Alto Firewall
3. **SNMPPORT** – The port at which the Palo Alto Firewall exposes its SNMP MIB; the default is 161.
4. **SNMPVERSION** – By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the **SNMPVERSION** list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **V3**, then select the corresponding option from this list.

5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear.
6. **USERNAME** – This parameter appears only when v3 is selected as the **SNMPVERSION**. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against the **USERNAME** parameter.
7. **CONTEXT** – This parameter appears only when v3 is selected as the **SNMPVERSION**. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the *SNMPEngineID* value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a *contextName*). If the **USERNAME** provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the **USERNAME** in the **CONTEXT** text box. By default, this parameter is set to *none*.
8. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the snmpversion selected is **v3**.
9. **CONFIRM PASSWORD**– Confirm the **AUTHPASS** by retyping it here.
10. **AUTHTYPE** – This parameter too appears only if **v3** is selected as the **SNMPVERSION**. From the **AUTHTYPE** list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options:
    - **MD5** – Message Digest Algorithm
    - **SHA** – Secure Hash Algorithm
11. **ENCRYPTFLAG** – This flag appears only when v3 is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option.
12. **ENCRYPTTYPE**– If the **ENCRYPTFLAG** is set to **YES**, then you will have to mention the encryption type by selecting an option from the **ENCRYPTTYPE** list. SNMP v3 supports the following encryption types:
    - **DES** – Data Encryption Standard
    - **AES** – Advanced Encryption Standard
13. **ENCRYPTPASSWORD** – Specify the encryption password here.
14. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.
15. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

16. **DATA OVER TCP –** By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the target firewall over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement unit	Interpretation
Active tunnels:	Indicates the number of tunnels that are currently active on the firewall using the GlobalProtect subscription.	Number	If the value of this measure is consistently high or if the value of this measure exceeds the maximum number of tunnels that are allowed, then administrators should analyze what exactly has increased the number of tunnels? - is the genuine user activity the real reason behind the increase in tunnels or is there any malicious activity or spam that is increasing the number of tunnels?
GlobalProtect gateway utilization:	Indicates the percentage utilization of the GlobalProtect gateway.	Percentage	A consistently high value for this measure is a cause of concern. Administrators should therefore consider increasing the number of GlobalProtect gateways.

2

Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to the **PaloAlto Network Firewall**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.