Hi

Hello! How can I assist you today?

while setting new firewall policy on my fortigate 80F, there is a setting: utm-status enable. What does it do?

The "utm-status enable" setting on a FortiGate firewall enables the inspection of network traffic using Unified Threat Management (UTM) features. UTM includes a set of security services that can be applied to network traffic passing through the firewall, such as antivirus, web filtering, intrusion prevention, and application control.

Enabling "utm-status" on a firewall policy means that the FortiGate will perform UTM checks on the traffic matching that policy. If UTM detects any malicious or suspicious activity, it can take actions such as blocking the traffic or alerting the administrator.

It's worth noting that enabling UTM features on a firewall policy can impact performance, especially on lower-end models like the FortiGate 80F. Therefore, it's important to carefully consider which UTM features to enable and their associated performance impact before enabling "utm-status" on a firewall policy.

thank you

You're welcome! If you have any more questions, feel free to ask.

Same question but for the setting: inspection-mode proxy, what does it do?

The "inspection-mode proxy" setting on a FortiGate firewall specifies that the firewall should use a proxy-based inspection method for the traffic matching that policy.

When a firewall policy is set to "inspection-mode proxy," the FortiGate firewall creates a proxy connection for each session that matches the policy. The firewall then inspects the traffic passing through the proxy, looking for any threats or suspicious activity.

This method of inspection allows the firewall to perform a more detailed inspection of the traffic than it can with other inspection modes like flow-based inspection. Proxy-based inspection is particularly useful for inspecting encrypted traffic, as it allows the firewall to decrypt the traffic, inspect it, and then re-encrypt it before forwarding it to its destination.

However, it's important to note that proxy-based inspection can be more resource-intensive than other inspection methods, which can impact firewall performance. Therefore, it's important to carefully consider the performance impact of using "inspection-mode proxy" before enabling it on a firewall policy.

ok, another one about the setting: set ssl-ssh-profile "certificate-inspection"

The "set ssl-ssh-profile" command on a FortiGate firewall is used to specify the SSL/SSH inspection profile to be used for traffic matching the policy. In this case, the SSL/SSH inspection profile being specified is "certificate-inspection."

When SSL/SSH inspection is enabled on a firewall policy, the FortiGate firewall inspects the encrypted traffic to ensure that it complies with security policies and does not contain any threats. The SSL/SSH inspection profile determines the level of inspection that will be performed on the traffic.

In the case of the "certificate-inspection" profile, the firewall will inspect the SSL/TLS certificate being used by the client and the server to establish the connection. This allows the firewall to verify that the certificate is valid and has not been tampered with, which can help prevent Man-in-the-Middle (MitM) attacks.

Enabling SSL/SSH inspection can impact firewall performance, especially on lower-end models. Therefore, it's important to carefully consider the performance impact of enabling SSL/SSH inspection and select the appropriate inspection profile for your needs.

another on, on the same device: what is the: set av-profile "default"?

The "set av-profile" command on a FortiGate firewall is used to specify the antivirus profile to be used for traffic matching the policy. In this case, the antivirus profile being specified is "default."

When an antivirus profile is applied to a firewall policy, the FortiGate firewall inspects the traffic passing through the policy for known viruses and malware. The "default" antivirus profile is a preconfigured profile that comes with the FortiGate firewall and is designed to provide basic antivirus protection.

The "default" antivirus profile includes virus signature-based detection, which involves comparing the traffic to a database of known virus signatures, as well as heuristic-based detection, which uses behavioral analysis to detect new and unknown viruses. The profile can also be configured to perform actions such as quarantining infected files or blocking traffic altogether.

It's important to note that while the "default" antivirus profile can provide basic protection, it may not be sufficient for all environments. Depending on your security requirements, you may need to customize the antivirus profile or use additional security measures to provide adequate protection against threats.

another one: what is the set ips-sensor "block-ips"?

The "set ips-sensor" command on a FortiGate firewall is used to specify the Intrusion Prevention System (IPS) sensor to be used for traffic matching the policy. In this case, the IPS sensor being specified is "block-ips."

When an IPS sensor is applied to a firewall policy, the FortiGate firewall inspects the traffic passing through the policy for known and unknown network-based threats such as malware, exploits, and other types of attacks. The "block-ips" IPS sensor is a preconfigured sensor that comes with the FortiGate firewall and is designed to provide a high level of protection by blocking known threats.

The "block-ips" sensor works by matching the traffic against a database of known signatures for known threats. If a match is found, the IPS sensor can take action, such as blocking the traffic or logging the event. The "block-ips" sensor can also be configured to detect and block new or unknown threats using behavior-based analysis.

It's important to note that while the "block-ips" sensor can provide a high level of protection against known threats, it may also generate false positives or false negatives. Therefore, it's important to carefully consider the security requirements of your environment and fine-tune the IPS sensor configuration to balance security and performance.

would you be able to summarise for me what services are available for a fortigate 80f without paid subscription, and the different services I could get with the different levels of subscriptions available?

Sure, here's a summary of the services available on a FortiGate 80F firewall without a paid subscription, as well as the different services that can be obtained with the various subscription levels:

Services available without a subscription:

* Firewall functionality, including NAT, routing, and basic security policies.
* VPN services, including IPsec, SSL VPN, and PPTP.
* Web filtering, with a limited set of predefined categories and URLs.
* Application control, with a limited set of predefined applications and categories.
* Basic antivirus protection, with the "default" antivirus profile.
* Basic IPS protection, with the "block-ips" IPS sensor.
* Limited logging and reporting functionality.

Subscriptions available:

* FortiGuard Antivirus Subscription: Provides regular updates to the antivirus database and advanced malware protection.
* FortiGuard IPS Subscription: Provides regular updates to the IPS database and advanced threat protection.
* FortiGuard Web Filtering Subscription: Provides access to a more extensive database of web filtering categories and URLs.
* FortiGuard Application Control Subscription: Provides access to a more extensive database of applications and categories.
* FortiGuard Security Rating Service Subscription: Provides a security rating score for each URL and IP address, based on its risk level.
* FortiGuard Industrial Security Service Subscription: Provides advanced security features for Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) environments.
* FortiAnalyzer Cloud Subscription: Provides advanced logging and reporting functionality in the cloud.
* FortiManager Cloud Subscription: Provides advanced centralized management functionality in the cloud.

It's important to note that while the basic services available without a subscription can provide some basic security functionality, the advanced subscription-based services are necessary to provide more comprehensive protection against the latest threats. Therefore, it's recommended to carefully evaluate your security requirements and consider subscribing to the appropriate services to ensure the best possible protection.