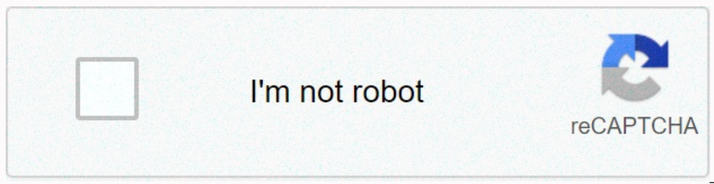

Continue

Fortinet utm protection datasheet

Fortinet offers a very robust UTM (Unified Threat Management) feature set that makes Fortinet-based hardware extremely powerful. A lot of firewall and router-based hardware is the ability to see applications that switch networks and make decisions based on this information, a lot of things that are missing these days and ages. Most firewalls are simple source/destination/port-based firewalls. They don't see dropbox being used or skype inging over the pipe. They only see the computers that start the traffic, the destinations they're going to, and the ports and services that are being used. Fortinet UTM Features allow users to see applications that pass through the network. This allows the administrator to decide whether to allow or deny traffic based on this new information. FortiGate's allows administrators to block Skype or allow it only for certain machines. It's an incredible force that gives a real fragment to what's about to cross your network. Not only does this enable application-based decisions to be made, but it also opens up web filtering, intrusion protection, data loss prevention, and ssl prevention cantes of worms. If you really want to know what's going on on your network and where the threats really are, Fortinet UTM is for you. The following sections separate UTM into the various security profiles that UTM provides and uses. Fortinet UTM Features From the FortiGate®-30 series to the FortiGate-5000 series for large businesses, service providers, and carriers, the FortiGate series brings together a range of security features to protect your network from threats. As a whole, these features are called Security Profiles when included in a single Fortinet security device. The Security Profiles included in your FortiGate model include: AntiVirus Anti-Attack System (IPS) Web filtering, including protection against Spam and grayware Data Leak Prevention (DLP) Application Control ICAP Firewall policies, while limiting access to e-mail filtering, while these and similar features are an important part of securing your network, but are not included in this document. This section includes the following topics: Traffic control Content control and filtering Security Profiles components Security Profiles/lists/sensors Traffic control When the FortiGate unit investigates network traffic one by one for IPS signatures, traffic analysis is performed. This is not content analysis where traffic is buffered until files, e-mail messages, web pages, and other files are put together and reviewed as a whole. DoS policies use traffic analysis by monitoring the type and quantity of packages, as well as their source and destination addresses. Application control uses traffic analysis to determine which application created the package. Traffic control does not include package pick-up and assembly, but packets can be broken into pieces as they pass from network to network. These parts are re-combined by the FortiGate unit before inspection. The two networks are not the same, and a few recommendations do not apply to all networks. This topic offers suggestions on how to use the FortiGate unit to help secure your network from content threats. IPS signatures IPS signatures can detect malicious network traffic. For example, the Code Red worm attacked a vulnerability on the Microsoft IIS web server. FortiGate's IPS system can detect traffic that is trying to exploit this vulnerability. IPS can also detect that infected systems communicate with servers to get instructions. Page 12 IPS recommendations Enable network-side IPS scanning for all services. Use FortiClient endpoint IPS scanning to protect against threats entering your network. Subscribe to FortiGuard IPS Updates and configure your FortiGate volume to receive push updates. This allows you to import new IPS signatures as soon as they are available. Your FortiGate volume contains IPS signatures written to protect certain software titles from DoS attacks. Enable signatures for the software you have installed and set the signature action to Block. You can view these signatures by going to Security Profiles > Attack Protection'> by predefined and sorting or filtering the group group, because it is very important to configure IPS signatures to protect against attacks on services that enable you to be monitored and to block matching signatures. For example, if you have a web server, configure the action of web server signatures as Blocking. Suspicious traffic attributes Network traffic itself can be used as an attack vector or as a tool to investigate a network before an attack. For example, the SYN and FIN flags should never appear together in the same TCP packet. When using the SYN flag to start a TCP session, the FIN flag shows the end of the data transfer at the end of a TCP session. The FortiGate volume has IPS signatures that recognize abnormal and suspicious traffic attributes. The SYN/FIN combination is one of the suspicious flag combinations detected by TCP in TCP traffic. Bad. FLAGS signature. Signatures created specifically to examine traffic options and settings begin with the name of the type of traffic they are associated with. For example, signatures created to examine TCP traffic have signature names that begin with TCP. Application control While applications can often be blocked by the ports they use, application control allows for convenient management of all supported applications, including those that do not use the ports set. Application control recommendations Some applications behave in an unusual way in terms of application control. For more information, see the App considerations page on page 144 By default, application control allows applications that are not specified in the application checklist. For high you may

want to change this behavior so that only explicitly permitted applications can be allowed. Content control and filtering When I search for fortiGate volume files, e-mail messages, web pages, and other similar files to re assembly before reviewing them, the content check performs. Traffic control is carried out by the FortiGate unit by examining individual packets of network traffic. The two networks are not the same, and a few recommendations do not apply to all networks. This topic offers suggestions on how to use the FortiGate unit to help secure your network from content threats. Before using suggestions, make sure you understand the effects of the changes. AntiVirus FortiGate antivirus scanner can detect viruses and other malicious loads used to transmitted machines. The FortiGate volume does deep content checking. The antivirus scanner will re-assemble fragmented files and remove compressed content to prevent attempts to hide viruses. The patented Compact Pattern Recognition Language (CPRL) increases the detection rates of virus variations in the future, ordering more control over common patterns. Antivirus recommendations Allow network-side antivirus scanning for all services. Use FortiClient endpoint antivirus scanning to protect against threats entering your network. Subscribe to FortiGuard AntiVirus Updates and configure your FortiGate volume to receive push updates. This allows you to get new antivirus signatures as soon as they are available. If your FortiGate volume supports it, enable the Extended Virus Database. Review antivirus logs regularly. Pay particular attention to repeated detections. For example, repeated virus detection in SMTP traffic may indicate that a system on your network is infected and is trying to communicate with other systems to spread the infection using a bulk mailer. The built-in patterns file filter list contains about 20 file delegations. Most represented files can be executed or opened by double-clicking. If any of these file patterns are not taken as part of your regular traffic, blocking them can help protect your network. This saves resources because blocked files do not need to be scanned for viruses. Avoid scanning e-mail messages twice to protect system resources. Scan and receive messages as they enter and exit your network, or when clients send and receive them instead. FortiGuard Web Filtering is the most popular part of the Web Internet, and as a result, almost any computer connected to the Internet can communicate using port 80, HTTP. Botnet uses this open port of communication and uses it to communicate with infected computers. FortiGuard Web Filtering from malware sites can help stop infections and prevent communication if an infection occurs. FortiGuard Web Filtering recommendations Enable FortiGuard Web activation on the edge of the network. Install FortiClient and use FortiGuard Web Filtering on systems that skip your FortiGate volume. Block categories such as Pornography, Malware, Spyware, and Phishing. These categories are more likely to be dangerous. Enable IP Address Control in FortiGuard E-mail Filtering in the e-mail filter profile. Many IP addresses used in spam messages lead to malicious sites; controlling them protects your users and your network. Email filter Spam is a common tool for delivering attacks. Users typically open email attachments that they shouldn't open and get infected with their own machines. The FortiGate email filter can detect and mark malicious spam, alerting the user to potential danger. E-mail filter suggestions Enable network-side e-mail filtering for all types of e-mail traffic. Use FortiClient endpoint scanning to protect against threats entering your network. Subscribe to the FortiGuard AntiSpam Service. DLP, most security features on the FortiGate volume are designed to keep unwanted traffic out of your network, while DLP can help prevent sensitive information from leaving your network. For example, credit vehicle D numbers and social security numbers can be detected by DLP sensors. DLP recommendations Rules for HTTP posts can be created, but if the requirement is to block all HTTP posts, a better solution is to use the application control or the HTTP POST Action option in the web filter profile. While DLP can detect sensitive data, blocking unnecessary communication channels is more effective than using DLP to examine. For example, if you use it for instant messaging or peer-to-peer communication in your organization, use application control to completely block them. Security Profiles components The AntiVirus Your FortiGate volume stores a virus signature database that can identify more than 15,000 individual viruses. FortiGate models that support additional virus databases can identify hundreds of thousands of viruses. With the FortiGuard AntiVirus subscription, signature databases are updated when a new threat is discovered. Antivirus also includes file filtering. When you specify files by type or file name, the FortiGate volume stops matching files from reaching your users. FortiGate volumes with a hard disk or configured to use the FortiAnalyzer unit can store infected and blocked files that you can review later. The Attack Protection System (IPS) FortiGate Attack Protection System (IPS) protects your network from hacking and other attempts to exploit your systems' security. More than 3,000 signatures can detect open lyses against various operating systems, host types, protocols, and applications. These can be stopped before they reach your internal network. You can also write custom signatures that are appropriate for your network. Web A Web filter contains a number of features that you can use to protect or limit the effectiveness of your users on the web. Contains. Web Filtering is a subscription service that allows you to limit access to websites. More than 60 million websites and two billion webpages are rated by category. You can choose to allow or block each of the 77 categories. URL filtering can prevent your network users from accessing the URLs you specify. Filtering web content may restrict access to webpages based on the words and phrases that appear on the webpage. You can create lists of words and phrases, each with points. When a web content list is selected in a web filter profile, you can specify a threshold. If a user tries to load a webpage and the score of words on the page exceeds the threshold, the webpage is blocked. Email filtering FortiGuard AntiSpam is a subscription service that includes an IP address blacklist, a URL blacklist, and an email check database. These resources are updated each time new spam messages are received, so you don't need to keep any lists or databases to ensure accurate spam detection. You can use your own ip address lists and email address lists to allow or reject addresses, depending on your needs and status. Data Leak Prevention (DLP) Data leak prevention allows you to define the format of sensitive data. The FortiGate volume can then monitor network traffic and prevent sensitive information from leaving your network. Includes rules for U.S. social security numbers, Canadian social insurance numbers, Visa, Mastercard, and American Express card numbers. Application Control You can block the use of some applications by blocking the ports they use for communication, but many applications do not use standard ports to communicate. Application control detects network traffic for more than 1,000 applications, collecting your control over application communication. ICAP This module allows certain processes to be emptied to a separate server so that your FortiGate firewall can optimize its resources and maintain the best possible level of performance. Security Profiles/lists/sensors A profile is a set of settings that you can apply to one or more firewall policies. Each Security Profile feature is enabled and configured on a profile, list, or sensor. They are then selected in a security policy, and the settings apply to all traffic that matches the policy. For example, if you create an antivirus profile that enables antivirus scanning of HTTP traffic, and you select the antivirus profile in the security policy that allows your users to access the World Wide Web, all web browsing traffic is scanned for viruses. Because you can use profiles in multiple security policyes, instead of repeatedly configuring the same profile settings for each security policy, a set of firewalls that require the same levels of protection and types you can configure a profile for the types of traffic processed by . For example, even though traffic between trusted and untrusted networks needs strict protection, moderate protection may be required between trusted internal addresses. To provide different levels of protection, you can configure two separate sets of profiles, one for traffic between trusted networks and one for traffic between trusted and untrusted networks. Security Profiles include: antivirus profile IPS sensor Web filter profile Email filter profile Data Leak Prevention profile Application Checklist VoIP profile Although they are called profiles, sensors, and lists, they are functionally equivalent. Each property is used to configure how it works. Pages: 1 2 3 4 5 6 7 8 9 10 11 12 13 14 Are you having trouble configuring your Fortinet hardware or have some questions to answer? Check out Fortinet Guru Youtube Channel! Do you want someone else to take care of it for you? Get some advice from Fortinet GURU! Don't forget to visit your YouTube Channel for the latest Fortinet Training Videos and Q&A sessions! - FortinetGuru YouTube Channel - FortiSwitch Training Videos Videos