Click to verify

Subsections 3.4.1 msg The msg rule option tells the logging and alerting engine the message to print along with a packet dump or to an alert. It is a simple text string that utilizes the \ as an escape character to indicate a discrete character that might otherwise confuse Snort's rules parser (such as the semi-colon ; character). 3.4.1.1 Format msg:""; 3.4.2 reference The reference keyword allows rules to include references to external attack identification systems. The plugin currently supports several specific systems as well as unique URLs. This plugin is to be used by output plugins to provide a link to additional information about the alert produced. Make sure to also take a look at for a system that is indexing descriptions of alerts based on of the sid (See Section). Table: Supported Systems System URL Prefix bugtraq cve nessus arachnids (currently down) mcafee osvdb msb url http:// 3.4.2.1 Format reference:, ; [reference:, ;] 3.4.2.2 Examples alert tcp any any -> any 7070 (msg:"IDS411/dos-realaudio"; \ flags:AP; content:"|fff4 fffd 06|"; reference:arachnids,IDS411;) alert tcp any any -> any 21 (msg:"IDS287/ftp-wuftp260-venglin-linux"; \ flags:AP; content:"|31c031db 31c9b046 cd80 31c031db|"; \ reference:arachnids,IDS287; reference:bugtraq,1387; \ reference:cve,CAN-2000-1574;) 3.4.3 gid The gid keyword (generator id) is used to identify what part of Snort generates the event when a particular rule fires. For example gid 1 is associated with the rules subsystem and various gids over 100 are designated for specific preprocessors and the decoder. See etc/generators in the source tree for the current generator ids in use. Note that the gid keyword is optional and if it is not specified in a rule, it will default to 1 and the rule will be part of the general rule subsystem. To avoid potential conflict with gids defined in Snort (that for some reason aren't noted it etc/generators), it is recommended that values starting at 1,000,000 be used. For general rule writing, it is not recommended that the gid keyword be used. This option should be used with the sid keyword. (See section) The file etc/gen-msg.map contains contains more information on preprocessor and decoder gids. 3.4.3.1 Format gid:; 3.4.3.2 Example This example is a rule with a generator id of 1000001. alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;) 3.4.4 sid The sid keyword is used to uniquely identify Snort rules. This information allows output plugins to identify rules easily. This option should be used with the rev keyword. (See section) 100 Reserved for future use 100-999,999 Rules included with the Snort distribution 1,000,000 Used for local rules The file sid-msg.map contains a mapping of alert messages to Snort rule IDs. This information is useful when post-processing alert to map an ID to an alert message. 3.4.4.1 Format sid:; 3.4.4.2 Example This example is a rule with the Snort Rule ID of 1000983. alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;) 3.4.5 rev The rev keyword is used to uniquely identify revisions of Snort rules. Revisions, along with Snort rule id's, allow signatures and descriptions to be refined and replaced with updated information. This option should be used with the sid keyword. (See section) 3.4.5.1 Format rev:; 3.4.5.2 Example This example is a rule with the Snort Rule Revision of 1. alert tcp any any -> any 80 (content:"BOB"; sid:1000983; rev:1;) 3.4.6 classtype The classtype keyword is used to categorize a rule as detecting an attack that is part of a more general type of attack class. Snort provides a default set of attack classes that are used by the default set of rules it provides. Defining classifications for rules provides a way to better organize the event data Snort produces. 3.4.6.1 Format classtype:; 3.4.6.2 Example alert tcp any any -> any 25 (msg:"SMTP expn root"; flags:A+; \ content:"expn root"; nocase; classtype:attempted-recon;) Attack classifications defined by Snort reside in the classification.config file. The file uses the following syntax: config classification: ,, These attack classifications are listed in Table . They are currently ordered with 4 default priorities. A priority of 1 (high) is the most severe and 4 (very low) is the least severe. Table: Snort Default Classifications Classtype Description Priority attempted-admin Attempted Administrator Privilege Gain high attempted-user Attempted User Privilege Gain high inappropriate-content Inappropriate Content was Detected high policy-violation Potential Corporate Privacy Violation high shellcode-detect Executable code was detected high successful-admin Successful Administrator Privilege Gain high successful-user Successful User Privilege Gain high trojan-activity A Network Trojan was detected high unsuccessful-user Unsuccessful User Privilege Gain high web-application-attack Web Application Attack high attempted-dos Attempted Denial of Service medium attempted-recon Attempted Information Leak medium bad-unknown Potentially Bad Traffic medium default-login-attempt Attempt to login by a default username and password medium denial-of-service Detection of a Denial of Service Attack medium misc-attack Misc Attack medium non-standard-protocol Detection of a non-standard protocol or event medium rpc-portmap-decode Decode of an RPC Query medium successful-dos Denial of Service medium successful-recon-largescale Large Scale Information Leak medium successful-recon-limited Information Leak medium suspicious-filename-detect A suspicious filename was detected medium suspicious-login An attempted login using a suspicious username was detected medium system-call-detect A system call was detected medium unusual-client-port-connection A client was using an unusual port medium web-application-activity Access to a potentially vulnerable web application medium icmp-event Generic ICMP event low misc-activity Misc activity low network-scan Detection of a Network Scan low not-suspicious Not Suspicious Traffic low protocol-command-decode Generic Protocol Command Decode low string-detect A suspicious string was detected low unknown Unknown Traffic low tcp-connection A TCP connection was detected very low 3.4.6.3 Warnings The classtype option can only use classifications that have been defined in snort.conf by using the config classification option. Snort provides a default set of classifications in classification.config that are used by the rules it provides. 3.4.7 priority The priority tag assigns a severity level to rules. A classtype rule assigns a default priority (defined by the config classification option) that may be overridden with a priority rule. Examples of each case are given below. 3.4.7.1 Format priority:; 3.4.7.2 Examples alert tcp any any -> any 80 (msg:"WEB-MISC phf attempt"; flags:A+; \ content:"/cgi-bin/phf"; priority:10;) alert tcp any any -> any 80 (msg:"EXPLOIT ntpdx overflow"; \ dsize:>128; classtype:attempted-admin; priority:10); 3.4.8 metadata The metadata tag allows a rule writer to embed additional information about the rule, typically in a key-value format. Certain metadata keys and values have meaning to Snort and are listed in Table . Keys other than those listed in the table are effectively ignored by Snort and can be free-form, with a key and a value. Multiple keys are separated by a comma, while keys and values are separated by a space. Table: Snort Metadata Keys Key Description Value Format engine Indicate a Shared Library Rule "shared" soid Shared Library Rule Generator and SID gidsid service Target-Based Service Identifier "http" Note: The service Metadata Key is only meaningful when a Host Attribute Table is provided. See Section for details on the Host Attribute Table. . 3.4.8.1 Format The examples below show an stub rule from a shared library rule. The first uses multiple metadata keywords, the second a single metadata keyword, with keys separated by commas. metadata:key1 value1; metadata:key1 value1, key2 value2; 3.4.8.2 Examples alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; \ metadata:engine shared; metadata:soid 3|12345;) alert tcp any any -> any 80 (msg:"Shared Library Rule Example"; \ metadata:engine shared, soid 3|12345;) alert tcp any any -> any 80 (msg:"HTTP Service Rule Example"; \ metadata:service http;) 3.4.9 General Rule Quick Reference Table: General rule option keywords Keyword Description msg The msg keyword tells the logging and alerting engine the message to print with the packet dump or alert. reference The reference keyword allows rules to include references to external attack identification systems. gid The gid keyword (generator id) is used to identify what part of Snort generates the event when a particular rule fires. sid The sid keyword is used to uniquely identify Snort rules. rev The rev keyword is used to uniquely identify revisions of Snort rules. classtype The classtype keyword is used to categorize a rule as detecting an attack that is part of a more general type of attack class. priority The priority keyword assigns a severity level to rules. metadata The metadata keyword allows a rule writer to embed additional information about the rule, typically in a key-value format. Snort 3 SNORT® Intrusion Prevention System, the world's foremost open source IPS, has officially launched Snort 3, a sweeping upgrade featuring improvements and new features resulting in enhanced performance, faster processing, improved scalability for your network and a range of 200+ plugins so users can create a custom set-up for their network. For more about Snort 3's improvements and new features, check out our quick breakdown here. This version of Snort was developed in close collaboration with the Snort community. The benefits of upgrading are readily apparent: Snort 3 is redesigned in C++ which makes the code base more modular and easier to maintain on your network. Threading and shared memory allow you to scale Snort 3 to your network and create a much faster start-up. This allows multiple packet processing to free up more memory for more packet processing power. Plugins with Luajit allows users to write their own plugins much easier than before to do things like add your own Snort Rule options, in-depth file processing, and more. Snort Rule Syntax has been updated to make it easier to write and to understand, especially for new users. The rule syntax is more concise with fewer rule parts which will allow rules to run quicker. Feature Snort 2 Snort 3 Packet threads One per process Any number per process Config memory use N processes * M GB M GB total, more for packets Config reload N processes, slower One thread that can be pinned to separate cores Startup Single-threaded, slower Multithreaded, faster Plugins Limited to preprocs and outputs Full plugin system with more than 200 plugins DAQ 2.X, run to completion 3.X, vector input, multiple outstanding packets DAQ modules Only legacy modules Stacked modules, IOCTLs, file, socket and text modules PCAP readback speed X Mbits/sec for Max-Detect 2X with AC, 4X with hyperscan IP layers Two max Arbitrary and configurable limits IP reputation Complex with shared memory Simplified process memory Stream TCP Complex implementation New and improved implementation Service detection AppID only, port configs required Autodetection, most port configs optional HTTP inspector Partly stateful Fully stateful Port scan detection High, medium and low thresholds only Fully configurable detection thresholds Config parsing Report one error and quit Report all errors Command line Some overlapping with config file Set to override any config file from the command line Default config Complex, needs tuning Simplified, effective Policy examples None Tweaks to fit all standard Talos policies Policy binding One level Nested Rule syntax Inconsistent and requires line escapes Uniform system with arbitrary whitespace Rule parsing Buggy with limited warnings Robust with numerous optional warnings Rule comments Comments only #, #begin/#end marks, C-style and rem options Alert file rules No Yes Alert service rules No Yes Fast-pattern buffers 6 available 14 available SO rule features Restricted functionality True superset of text rules Simple SO rules No Yes Dump built-in stubs No (SO stubs only) Yes Runtime tracing No (debug tracing and misc logs only) Yes Documentation LaTeX-based PDF, READMEs ASCII docs, text, HTML and PDFs Command-line help No Yes Source code 470,000 lines of C, with an average of 400 lines per file 389,000 lines of C++, with an average of 200 lines per file Distribution Snort.org tarballs, with updates coming every six months GitHub repo, with updates coming every two weeks This guide aims to assist Cisco Secure Firewall customers transitioning from Snort 2 to Snort 3. Snort 3 represents a significant update in both detection engine capabilities as well as the Firewall Management Center (FMC) intrusion policy user interface. While support for Snort 2 continues, Snort 3 will become the primary focus of new and improved threat detection features as the Secure Firewall product line advances. At the same time, some legacy Snort 2 features may not be supported in early Snort 3 versions. Because of this, customers must understand what to expect before deciding to move to Snort 3. We will start with a high-level comparison of the two Snort versions. Later, this document outlines the various Secure Firewall releases and the new Snort 3 features available in each. This is followed by a detailed discussion of what to expect when moving to Snort 3. The goal is to allow customers to determine when moving to Snort 3 becomes a viable option. Snort was originally written by Martin Roesch and began life as a network sniffer in 1998. In 1999, intrusion detection capability was added, making it one of the world's first Intrusion Detection Systems (IDS). Snort was very successful as an open-source project and became the core component of the new Sourcefire Intrusion Detection System when the company was formed in 2001. Inline capabilities were added in 2004 to provide Snort Intrusion Prevention System (IPS) capabilities. Now, Snort could detect and stop malicious network traffic. Historically network traffic speeds have grown faster than that of the computing systems running applications such as Snort. As a result, significant, ongoing development has improved the efficiency of Snort's deep packet inspection capability. These improvements and special high-speed device hardware have empowered Snort devices to perform intelligent deep packet inspection even at multi-gigabit network speeds. At the same time, Snort's abilities to detect and thwart evasion attempts have also grown. Network traffic consists of numerous encoding types, packet fragmentation, and reassembly. These, along with complex application and network protocols, offer attackers almost limitless opportunities to hide attacks. But as these opportunities have grown, so have Snort's capabilities. Purpose-built preprocessors normalize the various traffic types and protocols, removing obfuscations so Snort rules get an accurate picture of what the traffic really contains. Even with the many improvements, Snort developers realized they needed a better way to deal with network traffic flows. Snort 2 is packet-based, and many obfuscation techniques attempt to spread an attack across multiple packets. A better, flow-based detection engine was needed to overcome the inherent limits of packet-based inspection technology. After over a decade of development, Cisco released the Open Source version of Snort 3 in January 2021. The new Snort uses a flow-based detection engine. This new engine makes it much easier to normalize network traffic flows without overcoming Snort 2's packet-based limitations. Snort 3 preprocessors, now called inspectors, still serve a similar function, normalizing traffic for the rules engine. As part of the new Snort 3 flow-based detection, changes were also made to the interaction between the various data acquisition components on the Cisco Secure Firewall. These improvements have increased the overall inspection performance on Cisco devices without upgrading the hardware. This means that customers can increase existing device throughput capabilities simply by upgrading to the Snort 3 engine. One of the most anticipated features of Snort 3 addresses one of the most common complaints about Snort 2, its single-threaded nature. Snort 3 is now a multi-threaded process that consists of a single control thread and multiple detection processing threads. Figure 1: Snort 3 Architecture Snort 2, with its single-threaded design, required loading the configuration and network map separately for each process. Since Snort 3 does this once, it uses less memory, leaving the extra available for more IPS rules and/or a larger network map. There are several other changes and enhancements in Snort 3. Each is designed to address some of the weaknesses in Snort 2 and continue to improve on its already strong protection legacy. Figure 2 shows a quick summary, for more information visit www.snort.org. Figure 2: Snort 2 – Snort 3 Comparison Before deciding if you are ready to move to Snort 3, we need to understand the Secure Firewall software release strategy. Cisco follows a similar software release strategy as we have over the years with the Adaptive Security Appliance (ASA), consisting of short-lived and long-lived software releases. Releases come about every six months with alternating shorter and longer lifetimes. Most customers opt for long-term releases – denoted by even release numbers like 6.4, 6.6, 7.0, etc. Intermediate releases such as 6.5, 6.7, and 7.1 provide early access to new features for customers who need the most up-to-date software. Short-term releases typically include 18 months of software maintenance, while long-term and extra-long-term releases may be supported for 36 to 51 months after their initial release. All releases include 24 months of TAC support after software maintenance expires. See Figure 3 for an example of the software maintenance lifecycle. Figure 3: Software Maintenance Lifecycle For more information on Cisco's firewall software lifecycle, see the Firewall Product Line Software Release and Sustaining Bulletin. Cisco first introduced Snort 3 in the Cisco Firepower 6.7 release. This initial release was only available on devices managed locally using the Firepower Device Manager (FDM). Starting with release 7.0, Snort 3 was available on both FDM and FMC-managed devices. At its introduction, Snort 3 did not include all the features available in Snort 2. However, we are adding many of these features and more in subsequent 7.x software releases. The rest of this document applies only to FMC-managed devices. Information on the Firepower Device Manager. The following table outlines the features available in each release. The focus is on comparing functionality already available in Snort 2 to what this looks like in Snort 3. An empty cell indicates the feature is unchanged from the previous release. GUI policy editor New, faster GUI policy editor Search rules Similar rule searches using filter bar Set rule states to generate or drop and generate Similar, generate is now alert, drop and generate is now block Multiple additional rule actions available including: Block Drop Alert Rewrite Pass Reject Firepower Recommendations Not available, existing recommendations migrated as Snort 3 rule overrides during FMC upgrade Available, functionality largely the same as Snort 2 FMC Snort rule editor GUI Not available, custom Snort 3 rule text files can be uploaded to the FMC Custom Snort 3 rule text files can be uploaded to the FMC, rules can now be duplicated or edited in the FMC UI. Intrusion policy comparison report Not available Intrusion policy report Summary and overrides SNMP alerting for intrusion events Not available in intrusion policy, possible using FMC correlation rules Syslog alerting for intrusion events Available, setting moved to the AC policy Logging tab Sensitive Data preprocessor Custom sensitive data rules available, no sensitive data masking Rule dynamic state Not available Rate based rules Not available Rate_filter inspector available in custom Network Analysis policy Global rule threshold customization Not available, fixed at 60 sec Audit comments on intrusion policy changes Not available View new/changed rules in SRU View new/changed rules in LSP View intrusion rule from analysis packet view Available, shows Snort 2 rule when both Snort 2 and 3 rules exist for SID Intrusion event packet view Packet view/download includes select normalized fields not complete packet data Enable/disable/suppress/threshold from analysis packet view Available (7.0.1) Custom intrusion policy layers Not available Snort rule comments Available, associated with the policy instead of the rule Intrusion policy commit/discard Not available, policy changes are written immediately Intrusion policy locking No policy locking for multiple users Custom rule classifications Custom rules use built-in classifications or "unknown" classtype Rule suppressions for different intrusion policies Rule suppressions are per rule (apply to all policies). Existing suppressions are not migrated. Rule thresholds for different intrusion policies Rule thresholds are per rule (apply to all policies). Existing thresholds are not migrated. Portscan detection Available, ported from Snort 2 New, improved portscan detection/blocking Set rule state per policy Available, also can set rule states across multiple/all policies Import custom Snort rules Available, also convert custom Snort 2 to Snort 3 rules Rule download not available in Snort 2 Download custom Snort 3 rules Disable rule update for new SRU (LSP) Not Available Change base policy Available, also can customize security level per rule group Intelligent Application Bypass Available, however Snort 3 devices are limited to Drop Percentage and Flow Velocity thresholds only New Feature: Elephant flow visibility available only for Snort 3 devices New Feature: Encrypted Visibility Engine available only for Snort 3 devices Table 1: Snort 2 & 3 Feature Comparison Because of the Snort 3 Intrusion Policy user interface changes, it's essential to understand how your current policy management processes and procedures might translate from what you do today with Snort 2 to what this looks like for Snort 3. One of the most common administrative tasks is updating the Snort rule set. Talos rules are released twice a week as part of the normal release cycle and can also be released out of cycle for critical rule updates. The most common method for updating these is configuring the FMC to check for and download updates daily. This process is unchanged regardless of the Snort version on your managed devices. The rule update package for Snort 2 is the SRU or Security Rule Update. For Snort 3, this package is an LSP or Lightweight Security Package. The new package is more flexible and smaller in size. However, the method of downloading and deploying to devices is unchanged. You will see both the SRU and LSP versions displayed on the FMC on the System > Updates > Rule Updates tab. Figure 4: Rule Updates Until Snort 2 is entirely deprecated, the FMC will continue to download both the SRU and LSP rule update packages at the scheduled interval. Key takeaways: LSP replaces SRU Rule updates follow the same schedule and process from Snort 2 to Snort 3 Allow rules in the Access Control Policy are the primary method to enable Snort deep packet inspection on network traffic. This is done by specifying an Intrusion policy on the Inspection tab for an Allow rule. This behavior is unchanged for Snort 2 and Snort 3 devices. Each Intrusion policy consists of both Snort 2 and Snort 3 versions. When a policy is specified on the Inspection tab, the deployed version of the policy will correspond with the Snort engine on the target device. When you first upgrade your FMC to a Secure Firewall 7.x release, the existing Snort 2 Intrusion policies is used to create equivalent Snort 3 versions. Therefore, immediately following your FMC upgrade, the Snort 2 and Snort 3 versions of your policies are the same. However, if time has passed since this upgrade, and you have made modifications to your Snort 2 policies, you should synchronize these changes to your Snort 3 policies. You can do this manually or by using the policy synchronization feature. What does this mean to you? When migrating a device from Snort 2 to Snort 3, you should ensure that your Snort 3 Intrusion policy mirrors your Snort 2 policy. While there will not be an exact one-to-one match for Snort 2 and Snort 3 rules, you can use the policy synchronization feature to ensure the policies provide equal protection/detection. Figure 5: Policy Synchronization On FMC 7.x the information note shown above indicates you have Allow rules that specify a customized Intrusion policy. This note appears regardless of the policy synchronization status. Another important consideration is using URL or Application Identification rules within your Access Control policy. Normal rule processing is from top to bottom. As soon as a rule matches a given connection, the rule action is applied to the traffic (Trust, Allow, Block, etc.) and no further rules are evaluated. The exception is the Monitor action which allows the traffic to continue to be evaluated by subsequent rules. However, this is different if the Access Control rule contains an application or URL criteria. The system can make a rule matching decision based on the first packet for the other criteria such as zone, port, IP address, etc. However, identifying the application or URL in a connection requires one or more data packets to pass through the firewall as the application or URL is determined. Because of how Snort inspects traffic, these packets that pass before the application or URL are identified do not get evaluated by other rules in the policy. This means that if you have an Allow rule later in your rule set with an associated Intrusion policy, this rule will not evaluate the full packet stream. To address this behavior, the Access Control policy contains an Advanced setting called "Intrusion Policy used before Access Control rule is determined." This setting allows the user to select an Intrusion policy that will evaluate the traffic while an application or URL is being identified. Figure 6: Advanced Setting Because of the way Snort 3 performs inspection, this setting is more critical than it is for Snort 2. The use of application identification or URL rules in your Access Control policy has a greater potential to allow traffic to pass uninspected unless you specify an Intrusion policy in the Advanced setting mentioned above. As a result, you should ensure that any time you use an application or URL criteria in an Access Control rule, you select an Intrusion policy in the "Intrusion Policy used before Access Control rule is determined" under Network Analysis and Intrusion Policies on the Advanced tab. Key takeaways: Access Control rules do not need to be updated when upgrading to Snort 3. Ensure Snort 2 and Snort 3 policy versions provide the same level of protection/detection. If using application or URL rules, ensure you select an intrusion policy under the "Intrusion Policy used before Access Control rule is determined" setting. Intrusion policy configuration is where you will find the most significant changes between Snort 2 and Snort 3. This section covers the significant changes between the two versions. Rule States Snort 2 rule management mainly consists of setting the rule state. Snort 3 calls this rule action. Snort 2 rule states: Generate Events Drop and Generate Events Disable Snort 2 custom rules can also be created using the Pass action. To enable these rules in a policy, you would set the state to Generate Events. Available Snort 3 rule actions depend on the software release. Release 7.1 introduced additional rule actions. Snort 3 rule actions: Alert Block Drop* Rewrite* Pass* Reject* * Added in the 7.1 release Disable is not technically a rule action as it simply means the rule is not deployed in the policy. Searching Another change users may find involves rule searching. Snort 2 policy provides numerous ways to search rules. The filter panel to the left of the rule list contains categories such as: Rule Configuration Rule Content Category Classifications Microsoft Vulnerabilities Microsoft Worms Platform Specific Preprocessors Priority Rule Update Each category can be expanded to several sub options. Selecting items here populates the filter bar and filters the rule list based on the selected criteria. The Snort 3 policy interface does not include all of these rule search options. For example, Microsoft Worms, Platform Specific, Preprocessors, Priority and several other options are no longer available. However, the Snort 3 rule search bar conducts a more thorough Snort rule search that provides the ability to search for specific rule keywords, a feature not available for Snort 2 rule searches. Figure 7: Rule Search The key here is that rule searches operate differently between the two policy versions. It's possible that your favorite Snort 2 rule search may not work the same for Snort 3 rules. However, as you become familiar with the Snort 3 rule search feature, you will be able to locate the rules you are looking for - it just may take a little practice. Other Rule Settings There are a few other rule settings that have changed. Dynamic State, a seldom-used Snort 2 feature, is unavailable in Snort 3. Intrusion rules with dynamic states set will not be migrated to Snort 3 policies. Another deprecated feature is per rule SNMP alerting. While this is no longer available in the Intrusion policy, you can still create FMC Correlation rules to send SNMP traps for intrusion events generated by specific Snort rules. While supported on Snort 3, rule comments are not migrated from Snort 2 to Snort 3 rules. In addition, in Snort 3, comments are saved with the policy instead of the rule. Comments added to a rule in one policy will not be visible in other policies. When a policy is deleted, the associated rule comments are also removed. Custom Rules Snort 3 has a new rule syntax similar to Snort 2. The Snort 3 syntax has a few new keyword options and has removed many Snort 2 syntax inconsistencies. Because of this, the two rule languages are not compatible. Snort 3 also provides more flexibility for organizing custom rules. You can now create multiple custom rule groups that can be added to policies the same way as the system-created groups. A custom rule can be a member of one or more custom groups. The system provides a rule conversion utility to convert the syntax of your Snort 2 custom rules to Snort 3. For most Snort 2 rules, this works fine. However, you should be aware that while the Snort 3 rules will be syntactically correct, detection may not be identical between the two rule versions. You should evaluate your converted rules to ensure they have the same detection level as the originals. In fact, Talos recommends manually converting Snort 2 rules unless you have a large custom rule set, making manual conversion impractical. Also, manual rule conversion allows you to take advantage of the new keyword options if desired. One issue that can occur with Snort 2 to 3 conversion is failing to specify inspection buffers. In Snort 2, if the rule does not contain buffer information, Snort will still inspect the raw packet data. However, in Snort 3, if a buffer exists for the normalized flow data, then that data will not be available in the raw packet. The example Snort 2 rule below will trigger on a Snort 2 device:alert tcp $EXTERNAL_NET any -\> $HOME_NET $HTTP_PORTS (msg:"HTTP rule without proper URI buffer"; flow:to_server,established; content:"/myurl"; classtype:misc-activity; sid:1000000;) The converted Snort 3 rule is exactly the same as above. No syntax changes are required in this case. However, because we have a buffer available for the HTTP URI, the Snort 3 rule will not inspect this in the raw packet data, and the rule will not trigger. Adding the proper buffer to the Snort 3 rule might look like this:alert tcp $EXTERNAL_NET any -\> $HOME_NET $HTTP_PORTS (msg:"HTTP rule with proper URI buffer"; flow:to_server,established; http_uri; content:"/myurl"; service:http; classtype:misc-activity; sid:1000000;) Note the addition of the http_uri and service:http keywords. If the original rule had followed proper rule-writing practices, both of these (in their Snort 2 equivalents) would have been in the Snort 2 version of this rule. If that were the case, the rule conversion – and Snort 3 detection - would have worked seamlessly. You can now use new Snort 3 features like the rem keyword to add a remark to a rule. You can also add C-style inline comments using /* and */ within your custom rules. alert http (msg:"HTTP URL rule"; flow:to_server,established; http_uri; content:"/myurl"; classtype:misc-activity; rem: "This rule doesn't need the service keyword since http is in the header"; /* This is a longer inline comment which can also be multi-line */ sid:1000000;) These are just a few of the many new features in the Snort 3 rules language. For more information, see www.snort.org or the Cisco Secure Firewall YouTube channel. The Firepower Recommendations feature was unavailable in the first Snort 3 capable release (7.0) but returned in the 7.1 and following releases. Also note that the name changed as of release 7.2 where the term Firepower was removed from the name of the feature, from 7.2 forward it's just Recommendations. Understanding how Recommendations are migrated between releases is a bit complex. Let's break it down by the various upgrade scenarios. Upgrade from 6.x to 7.0 and Remaining on Snort 2 If you do not plan to use Snort 3 on the 7.0 release, you don't need to take any action regarding Recommendations. If you are currently using Recommendations in your Snort 2 policies, these recommended rule states will be migrated to the Snort 3 versions as manual overrides. This happens on the FMC when you upgrade from 6.x to 7.0. It will also happen if you synchronize the intrusion policies manually following a 7.0 upgrade. In addition, rules with manually enabled/disabled rule states are also migrated to the Snort 3 policy. This means you will likely end up with a large number of rule overrides in your Snort 3 policy. That's ok because these will be addressed on your next upgrade to release 7.1 or greater. Upon upgrading from 7.0 to 7.1 or greater, the system will recognize the overrides added to your Snort 3 policies as a result of Recommendations. During the upgrade process, you will have the opportunity to remove these overrides. This will revert your Snort 3 policies to only keeping the actual manual overrides from their Snort 2 equivalents. After upgrading, you can then re-run recommendations in your Snort 3 policies if desired. Upgrade from 6.x to 7.0 and Moving to Snort 3 If you plan to upgrade to the 7.0 release and migrate to Snort 3, you will not be able to take advantage of Firepower Recommendations. You have two options, 1) remove Recommendations from your Snort 2 policies before upgrading 2) allow your current Snort 2 Recommendations to be migrated to Snort 3 as rule overrides. Each of the options above has some considerations. You will have to select the best one according to the requirements of your environment. Option 1: Remove Recommendations prior to upgrading to 7.0 Removing Recommendations means you lose the benefits of automatic policy customization. You cannot simply re-run Snort 2 Recommendations and re-synchronize your policies. You may want to evaluate the existing recommendations in Snort 2 and decide if you want to manually change some of the rule states in your Snort 3 policies. It means you will have to take a more active role in deciding which rules to enable/disable. You should also revisit this periodically as new rules are added through LSP updates. Option 2: Allow the system to migrate your Recommendations to your Snort 3 policies If you allow the system to migrate your Recommendations as overrides, you will start out with Snort 3 policies equivalent to their Snort 2 versions. However, over time the Snort 3 Recommendation overrides will not be automatically updated even if you re-synchronize your Snort 2 policies. The assumption here is that you have been regularly updating your Snort 2 Recommendations which is a recommended best practice. This means your Snort 2 and Snort 3 policies will begin to diverge as you continue to update Snort 2 Recommendations which are not migrated to your Snort 3 policies. The good news is once you upgrade again to a release that supports Recommendations (7.1 or higher) the system will allow you to back out the Recommendations overrides that were migrated. You can then configure and update Recommendations in your Snort 3 policies. Due to the way Recommendations work on Snort 2, additional rules enabled in a policy are always set to Generate Events (Alert action for Snort 3). This means the migrated Recommendation overrides present in the Snort 3 policy will always use Alert as the enabled rule action or Disabled if Recommendations is configured to disable rules. Upgrade from 6.x to 7.1 or Higher Releases For the 7.1 and higher releases, Recommendations are supported on Snort 3. Existing Snort 2 Recommendations will not be migrated to the Snort 3 versions of your policies. After upgrading, you can enable Recommendations in much the same manner as before. While the user interface is new, the process and outcome of running Recommendations are the same (only faster). Figure 8: Rule Recommendations Intrusion policy Advanced Settings are not available in Snort 3. However, just because there are no Advanced Settings doesn't mean that all of these features are unavailable. These include: Sensitive Data Detection Global Rule Thresholding SNMP Alerting Syslog Alerting For Sensitive Data Detection, custom Snort 3 rules can be created using the sd_pattern keyword. There is no need to enable anything specific to provide this detection. These rules can detect built-in patterns like U.S. Social Security numbers with or without dashes, credit card numbers, and custom regex patterns. The main difference in Snort 3 is that there is no option to mask sensitive data in captured packets matching these rules. Snort 3 Sensitive Data rule examples:alert tcp (msg:"SENSITIVE-DATA Credit Card Numbers"; sd_pattern:"credit_card",threshold 20; service:ftp-data,http,imap,pop3,smtp; sid:1200011;) alert tcp (msg:"SENSITIVE-DATA Email Address"; sd_pattern:"^\S+@\S+\.\S+$",threshold 20; service:ftp-data,http,imap,pop3,smtp; sid:1200012;) alert tcp (msg:"SENSITIVE-DATA U.S. Phone Numbers"; sd_pattern:"^[(]?\d{3}[)]?[(\s)?.-]\d{3}[\s.-]\d{4}$",threshold 20; service:ftp-data,http,imap,pop3,smtp; sid:1200013;) alert tcp (msg:"SENSITIVE-DATA U.S. Social Security - without dashes"; sd_pattern:"us_social_nodashes",threshold 20; service:ftp-data,http,imap,pop3,smtp; sid:1200014;) alert tcp (msg:"SENSITIVE-DATA U.S. Social Security - with dashes"; sd_pattern:"us_social",threshold 2; service:ftp-data,http,imap,pop3,smtp; sid:1200015;) alert http (msg:"Custom SD Pattern"; sd_pattern:"\d\d\d{2}", threshold 4; sid:1200016;) These are examples only and should not be used in a production environment. Global Rule Thresholding is enabled by default in both Snort versions. This threshold limits intrusion rule alerting to one alert every 60 seconds per rule, per destination IP address. In Snort 2, this threshold can be adjusted or disabled. Snort 3 uses a fixed threshold. As previously mentioned, SNMP alerting is not available in Snort 3 Intrusion policies. Still, you can create Correlation rules on your FMC to send SNMP alerts for specific Snort rules if desired. Syslog alerting moved in release 7.0 from the Intrusion policy to the Access Control policy Logging tab. The functionality remains the same, but it can now be configured for both Snort version policies there. User-created layers are not available for Snort 3 policies. While some of the built-in layers will return in later releases (Base Layer, Group Overrides, Recommendations, User Overrides), adding additional custom layers will not. You may be able to retain some of this functionality by using a custom policy as the Base Layer for another policy. However, if you regularly create new custom layers and merge layers, a new procedure will be required to replace this functionality as it is not planned for any subsequent releases. You should also be aware of a few changes to how policy editing works. When editing a policy, changes are committed as soon as they are made in the user interface. There is no Save or Commit button. This means there is no easy way to back out recent changes or discard edits before they are written to the policy. As a result of the change above, you can no longer add audit comments to a policy change. Changes to Snort 3 Intrusion policies are tracked on a per-change level in the audit log. Audit log entries give details about who made the change, which policy, and the modified rule. Figure 9: Audit Log Figure 10: Intrusion Policy Version Intrusion policy comparison reports are not available for Snort 3 policies. Also, Intrusion policy reports are generated for the Snort 2 and Snort 3 versions of the policy. However, the Snort 3 report contains only policy summary information and details on group and rule user overrides. Figure 11: Snort 2 Policy Comparison There is also no multi-user locking or notification on Snort 3 Intrusion policies. Users should ensure that multiple administrators do not simultaneously edit the same Intrusion policy rules. However, one advantage to this is that multiple administrators can now work on different parts of the same policy simultaneously. You may have noticed that after you first upgrade to a 7.x software release, each of your Intrusion policies has a synchronization status icon below it. If you don't have any custom Snort rules this icon will probably be green. Policy Synchronization Status This indicates that the Snort 3 version of the policy is in sync with the Snort 2 version. There will likely be a few less rules in the Snort 3 policy due to some of the consolidation between rule sets, but the protection level will be the same. If a policy is out of sync you will see an orange arrow below the policy name. Out of Sync Policies Clicking the orange arrow will bring up the synchronization summary. Synchronization Summary There are two important items to note about this synchronization feature. First, it was designed to be run just prior to moving to Snort 3 on your devices. The goal is it to take the current state of the Snort 2 policy and replicate that to the Snort 3 policy. After this, the idea is that you stop modifying the Snort 2 policy and only update the Snort 3 policy. This feature was not meant as a way for you to continuously keep the policies in sync as you maintain a hybrid Snort 2 and Snort 3 environment. Second, the synchronization is one way, Snort 2 -> Snort 3. In addition, changes to the Snort 3 policy are not tracked. Once the policies are in sync, if you change rule states in your Snort 3 policy, the synchronization state will remain green. In short, this is not a reliable way to tell if your policies are the same, it only shows if you have changed your Snort 2 policy. There have been some significant changes to editing the Network Analysis Policy in Snort 3. Besides the considerable UI changes, the policy itself has changed as well. Instead of preprocessors, the Snort 3 policy uses inspectors. These provide much of the same features and functions as their Snort 2 counterparts. Because of the architectural differences between Snort 2 and 3, the upgrade process will not attempt to migrate or translate these settings. One change you may note is that the Normalizer (Inline Normalization) Inspector is enbled in all Talos Network Analysis policies. In addition, these poicies are all in Prevention mode as opposed to Detection mode. It is important that users do not change these settings before consuting with TAC. Because of the differences in Snort 3 processing, disabling the Normalizer or changing the policy mode can have serious unintended consequences. After upgrading your FMC to a 7.x release, any customizations to your Network Analysis policies will not be present in the Snort 3 equivalent policies. Instead, you will see policies using default base settings depending on which Talos policy was used. Migrating any settings is a manual process if you have changed the Snort 2 version of these policies and want to incorporate those into the Snort 3 versions. Each Network Analysis policy is tailored and tested to work with its associated Talos Intrusion policy. In many cases, we have found that previous Snort 2 policy changes do not apply to Snort 3 because of the differences in how it processes traffic. This will be an opportunity for many customers to revert to a Talos-provided configuration that improves both efficiency and efficacy. Unless you have made significant changes to your Snort 2 Network Analysis policy, it is unlikely that this policy will present any issues or roadblocks upgrading to Snort 3. There are no changes between Snort 2 and Sort 3 for Malware & File, SSL, Network Discovery, Correlation, Prefilter, Identity or DNS policy. For more information about the Cisco Secure Firewall, please see the following resources: YouTube Snort 3 Playlist. In addition to the above information, you should carefully read the Release Notes and pay attention to any relevant information such as corrected or known defects. Cisco CX Services also offers a bug scrub service providing a customized and comprehensive defect search for a specific release. Contact your Cisco sales team for more information. Selected Defects The following defects may be of concern for some customers. This list is not inclusive of all defects in this release. Please consult the 7.0 Release Notes. Defect Title: Firepower release 7.0.x does not support ssl_state or ssl_version keywords for Snort 3 Defect ID: CSCwa16654 Symptom: Intrusion rules with the ssl_state and ssl_version keywords do not trigger when using Snort 3. Conditions: This defect exists for all 7.0 versions when Snort 3 is in use. Severity: 3 (moderate) Additional Info: The ssl_state and ssl_version keywords are used in Snort rules to identify the TLS handshake state and the TLS version in a connection. These keywords are used in various Snort rules created by Cisco Talos as well as third party/custom rules. Talos base policy rule sets include active rules using these keywords. Typical usage is shown below. ssl_state:client_hello; - identify a client Hello request to a server ssl_state:server_hello; - identify a server hello response ssl_state:server_keyx; - identify a server key exchange response ssl_version:tls1.2; - identify a TLS 1.2 connection Cisco Secure Firewall release 7.0.x does not support the use of these keywords in Snort 3 rules. The impact of this condition is that rules containing these keywords will not trigger - they will not generate alerts or block traffic. No errors will be generated when rules containing these keywords are created, uploaded or deployed to devices running Snort 3. Because of this, it may not be apparent to users that these rules are non-functional. Table 2: Release 7.0 Selected Defects Selected Defects The following defects may be of concern for some customers. This list is not inclusive of all defects in this release. Please consult the 7.1 release notes. Defect Title: Snort 3 client_hello keyword not working when SSL policy is in use Defect ID: CSCvz93449 Symptom: Intrusion rules with the client_hello keyword do not trigger when using SSL policy with Snort 3. Conditions: Release 7.1, intrusion policy deployed with rules using the client_hello keyword, Snort 3 is in use. Severity: 3 (moderate) Additional Info: Currently when the SSL inspector decides not to decrypt flows, because a policy configuration has decided not to decrypt, or possibly also because an error path was taken, "stop_inspection" is immediately called so further packets are not inspected by snort. However, it's possible there's a need for some customers to inspect encrypted flows. The client_hello IPS rule configuration lets a user inspect encrypted flows without decryption. This use case will not work if there is an SSL policy added on the device. Talos rules containing these keywords: client_hello: 70 Table 3: Release 7.1 Selected Defects Snort ist ein Open-Source-System zur Erkennung und Prävention von Netzwerkintrusion (IDS/IPS), das den Netzwerkdatenverkehr überwacht und potenziell bösartige Aktivitäten in IP-Netzwerken erkennt. Unternehmen können Snort mithilfe einer regelbasierten Sprache implementieren, die protokoll-, signatur- und anomaliebasierte Untersuchungsmethoden kombiniert, um bösartige Pakete im Netzwerkverkehr zu erkennen und potenzielle Angriffsvektoren zu blockieren.Auf die Mischung kommt es an. Gängige signaturbasierte Methoden sind bei der Erkennung bekannter Bedrohungen wirksam, bei unbekannten Bedrohungen sind sie jedoch nicht so gut geeignet. Snort nutzt auch verhaltensbasierte Ansätze, um tatsächliche Schwachstellen zu entdecken, indem es die Netzwerkaktivität mit einem vordefinierten Satz von Snort-Regeln vergleicht. Dadurch ist es in der Lage, komplexe zukünftige Bedrohungen zu erkennen, die durch signaturbasierte Methoden allein bisher möglicherweise nicht zu identifizieren waren.Anwendungsszenarien für SnortSnort wird hauptsächlich von Unternehmen verwendet, die ein plattformunabhängiges IDS/IPS suchen, um ihre Netzwerke vor zukünftigen Bedrohungen zu schützen. Folgende Aspekte geben den Ausschlag für Snort:Überwachung des Netzwerkverkehrs in EchtzeitProtokollanalyseInhaltsabgleich; gleicht Regeln nach Protokoll, Ports und dem Vorhandensein von Inhalt abFingerabdruck des Betriebssystems (BS)Kompatibilität mit beliebigem BSAber Snort hat noch mehr zu bieten.Paket-Sniffing und ProtokollierungSnort kann als Paket-Sniffer dienen, der den Netzwerkverkehr auf einer lokalen Netzwerkschnittstelle erfasst. Sie können Snort auch als Paketlogger nutzen, der erfasste Pakete auf die Festplatte schreibt, um den Netzwerkverkehr zu debuggen. Oder nutzen Sie die Netzwerk-IDS/IPS-Funktionen, um den Netzwerkverkehr in Echtzeit zu überwachen und jedes Paket auf verdächtige Aktivitäten oder potenziell bösartige Nutzlasten zu untersuchen.Warnungen und RegelnSnort kann basierend auf den konfigurierten Regeln Warnungen für alle ungewöhnlichen Pakete generieren, die im Netzwerkdatenverkehr entdeckt werden. Das kann helfen, Netzwerkbedrohungen oder andere Risiken zu identifizieren, die zur Ausnutzung von Schwachstellen führen könnten.Die Snort-Regelsprache ist sehr flexibel und ermöglicht Ihnen die Erstellung eigener Snort-Regeln, um regelmäßige Netzwerkaktivitäten von anormalen Aktivitäten zu unterscheiden. Dadurch können Sie neue Verfahren hinzufügen, die Snort anweisen, das Netzwerk auf bestimmtes Verhalten zu überwachen und potenzielle Angriffe auf das Netzwerk des Unternehmens zu verhindern.AngriffserkennungAufgrund der Flexibilität der Snort-Regelsprache und der Kompatibilität mit allen Betriebssystemen ist Snort in der Lage, jeden netzwerkbasierten Angriff zu erkennen, sofern dem Angriffsverhalten eine Regel zugeordnet ist. Im Folgenden sind einige Arten von Kompromittierungen aufgelistet, bei deren Erkennung Snort die Unternehmen unterstützen kann.DoS (Denial-of-Service)/DDoS (Distributed-Denial-of-Service)Bei DoS-/DDoS-Angriffen wird ein Netzwerk mit unzulässigen Serviceanfragen überflutet, um den Geschäftsbetrieb zu stören. Während ein DoS-Angriff von einem einzelnen System aus gestartet wird, handelt es sich bei einem DDoS-Angriff um einen orchestrierten Angriff, der von mehreren Systemen an mehreren Standorten ausgeht.PufferüberlaufEin Pufferüberlauf tritt auf, wenn der Angreifer mehr eingehenden Datenverkehr an eine Netzwerkadresse weiterleitet, sodass das Netzwerkdatenvolumen die gesamte verfügbare Bandbreite im System übersteigt.SpoofingManchmal imitiert ein Hacker einen autorisierten Benutzer oder ein autorisiertes System, um auf ein Zielnetzwerk zuzugreifen und Informationen zu stehlen oder böswillige Aktivitäten auszuführen. Das wird als Spoofing-Angriff bezeichnet.Common Gateway Interface (CGI)CGI stellt eine Schnittstelle zwischen Web und Endbenutzer zum Rendern dynamischer Webseiten bereit. Allerdings ist auch bekannt, dass es Sicherheitslücken enthält, die von Hackern ausgenutzt werden können. Webbasierte CGI-Skripte können häufig Opfer von Eingabevalidierungsangriffen werden, da bösartige Eingaben nicht gefiltert werden.Stealth-Port-ScansHacker verwenden häufig Stealth-Port-Scans, auch bekannt als halboffene Scans, um über offene Ports im Netzwerk anzugreifen, ohne eine vollständige Verbindung herzustellen. Dabei wird ein einzelnes Paket über den Drei-Wege-Handshake des Transmission Control Protocol (TCP) gesendet, und der Vorgang wird beendet, sobald ein Port im Zielnetzwerk erkannt wird. Dadurch werden Firewalls umgangen, und der Scan erscheint als normaler Netzwerkverkehr.Funktionsweise von SnortSnort basiert auf der Paketerfassungsbibliothek (libpcap), einer systemunabhängigen Schnittstelle zur Erfassung des Datenverkehrs, die in Netzwerkanalyseprogrammen weit verbreitet ist. Snort überwacht den Netzwerkverkehr und vergleicht ihn mit einem Snort-Regelsatz, der von Benutzern in einer Konfigurationsdatei definiert wird. Diese Regeln werden auf Pakete im Netzwerkverkehr angewendet, und Warnungen werden ausgegeben, wenn ungewöhnliche Aktivitäten erkannt werden.Wir möchten etwas genauer auf die Funktionsweise und Regeln von Snort eingehen.Snort-ModiSnort kann mit einem von drei Flags konfiguriert werden, die den Betriebsmodus bestimmen:Sniffer-Modus (Flag -v): Snort liest die TCP/IP-Pakete und gibt in der Konsole Paketinformationen aus.Paketprotokollierungsmodus (Flag -l): Snort protokolliert eingehende TCP/IP-Pakete zur weiteren Analyse in einem Protokollierungsverzeichnis auf der Festplatte.NIDS-Modus (Flag -c): Snort bestimmt anhand des in der Konfigurationsdatei angegebenen Regeltyps, ob eine Aktion für den Netzwerkverkehr ausgeführt werden soll.Snort-RegeltypenSnort wertet Regeln nicht in der Reihenfolge aus, in der sie in der Konfigurationsdatei aufgeführt sind. Stattdessen werden sie anhand des Regeltyps überprüft, der die Aktion angibt, die ausgeführt werden soll, wenn Snort ein Paket erkennt, das den Regelkriterien entspricht.Die fünf Grundregeltypen in Snort lauten:Warnregeln: Wenn ein verdächtiges Paket erkannt wird, generiert Snort eine Warnung.Blockierungsregeln: Snort blockiert das verdächtige Paket und alle nachfolgenden Pakete im Netzwerkfluss.Drop-Regeln: Snort verwirft das Paket, sobald die Warnung generiert wird.Protokollierungsregeln: Snort protokolliert das Paket, sobald die Warnung generiert wird.Bestanden-Regeln: Snort ignoriert das verdächtige Paket und markiert es als bestanden.Verständnis von Snort-RegelnEs ist wichtig, die Snort-Regeln richtig zu schreiben, damit sie wie vorgesehen funktionieren. Das heißt, dass sie zukünftige Bedrohungen in Ihrem Netzwerk erfolgreich identifizieren können. Dazu benötigen Sie ein klares Verständnis der Snort-Syntax und der Bildung der Regeln.Snort-Regeln werden zwar normalerweise in einer einzigen Zeile geschrieben, doch neuere Versionen von Snort ermöglichen auch mehrzeilige Regeln. Das ist besonders nützlich für komplexere Regeln, die sich nur schwer auf eine Zeile beschränken lassen.Snort-Regeln bestehen aus zwei logischen Teilen: Regelheader und Regeloptionen. Sehen wir uns das genauer an.RegelheaderDiese definieren die Aktion, die ausgeführt werden soll, wenn Datenverkehr identifiziert wird, der der Regel entspricht. Ein Regelheader besteht aus fünf Hauptkomponenten:Auszuführende Aktion: Die erste in einer Snort-Regel deklarierte KomponenteIP-Adressen: Quelle und ZielPortnummern: Quelle und ZielVerkehrsrichtung: -> für unidirektional von der Quelle zum Ziel; für bidirektionalPrüfprotokoll: Protokolle "Layer 3" (IP und ICMP) und "Layer 4" (TCP und UDP)Hinweis: Snort unterstützt derzeit zwar Layer 3 und 4, in Snort 3 können Sie Snort aber auch anweisen, Regeln nur mit dem Datenverkehr für den jeweiligen Anwendungsschicht-Service (z. B. SSL/TLS und HTTP) abzugleichen.RegeloptionenDiese definieren die Kriterien für den Netzwerkverkehr, die erfüllt sein müssen, damit eine Regel übereinstimmt, sowie die Ausgabe, wenn eine Übereinstimmung vorliegt. Hier sind einige der verfügbaren Regeloptionen:Meldung, die angezeigt wird, wenn die Regel übereinstimmt: Erläutert den Zweck der RegelFlussstatus: Gibt die Sitzungseigenschaften an, die für ein bestimmtes Paket überprüft werden sollenInhalt oder Muster: Gibt den Inhalt oder das Muster an, nach dem in den Payload- oder Nicht-Payload-Daten eines Pakets gesucht werden sollDienst- oder Anwendungsprotokoll: Weist Snort an, den Inhalt oder das Muster entweder im Datenverkehr des angegebenen Anwendungsschicht-Service oder an den im Regelheader angegebenen Quell- und Zielports zu identifizierenSnort-ID (Sid) und Revisionsnummer (Rev): Identifiziert eindeutig eine Snort-Regel (Sid) oder die Revisionsnummer einer Snort-Regel (Rev)Snort-BeispielregelnSehen wir uns an, wie Sie Snort-Regeln für einen DoS-Angriff mithilfe von Docker-Honeypots schreiben würden.Um diesen Angriffsmodus aufzudecken, müssen wir eine Regel schreiben, um HTTP-Anfragen zu erkennen, die von einem kompromittierten Docker-Image über eine TCP/IP-Verbindung gesendet werden:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTSDoS-Angriffe werden gestartet, indem der Server über eine bestehende Verbindung mit HTTP-GET-Anfragen überschwemmt wird. Daher müssen wir Snort anweisen, im Abschnitt für Regeloptionen nach diesem Muster zu suchen:# only detect established TCP connections from client requestsflow:to_server, established;# match on HTTP GET requestshttp_header; content:"Mozilla/5.0 (Windows NT 10.0|3B| Win64|3B| x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36";http_method; content:"GET";Da der Angriffsmodus über Honeypots gestartet wird, wird die Regel als Netzwerktrojaner-Aktivität klassifiziert:alert tcp $HOME_NET any -> $EXTERNAL_NET $HTTP_PORTS (msg: "Detects DoS HTTP request sent by compromised Docker image";flow:to_server, established;http_header; content:"Mozilla/5.0 (Windows NT 10.0|3B| Win64|3B| x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/98.0.4758.102 Safari/537.36";http_method; content:"GET";classtype:trojan-activity;sid:8001951;rev:20220420;)Einsatz von Snort-Regeln, die von Experten verfasst wurdenDie Implementierung von Snort in Ihren Cybersicherheits-Stack bietet einen flexiblen und plattformunabhängigen Ansatz zum Schutz Ihres Netzwerks vor bekannten und zukünftigen Bedrohungen der Netzwerksicherheit. Allerdings müssen die Regeln konfiguriert werden, damit sie ordnungsgemäß funktionieren.Für relativ einfache Anwendungsfälle könnten Sie Ihre eigenen Snort-Regeln schreiben, es ist jedoch eine anspruchsvolle Aufgabe, die Regeln im Hinblick auf zukünftige Bedrohungen auf dem neuesten Stand zu halten. Erwägen Sie stattdessen die Verwendung von Snort- und YARA-Regeln, die von Experten erstellt wurden, wie dem frei verfügbaren Community-Regelsatz oder CrowdStrike Falcon Intelligence. Lint line:

```
sudo /opt/snort/bin/snort --daq-dir=/opt/snort/lib/daq --plugin-path=/opt/snort/etc/rules/so_rules -c /opt/snort/etc/snort.lua -T pulledpork.conf: community_ruleset = false registered_ruleset = false LightSPD_ruleset = true oinkcode = redacted snort_blocklist = false et_blocklist = false #blocklist_path =
/opt/snort/etc/rules/lists/default.blocklist ips_policy = balanced rule_mode = simple rule_path = /opt/snort/etc/rules/snort-pulledpork.rules ignored_files = includes.rules, snort3-deleted.rules include_disabled_rules = false sorule_path = /opt/snort/etc/rules/so_rules/ distro = ubuntu-x64 snort_path = /opt/snort/bin/snort CONFIGURATION_NUMBER =
3.0.0-BETA ips entry in snort.lua: ips = { rules = [[ include /opt/snort/etc/rules/snort-pulledpork.rules ]], variables = default_variables } /opt/snort/etc/rules/so_rules dir: -rw-r--r-- 1 root root 21712 Aug 5 15:19 browser-chrome.so -rw-r--r-- 1 root root 17664 Aug 5 15:19 browser-ie.so -rw-r--r-- 1 root root 59000 Aug 5 15:19 browser-other.so -rw-r--r-- 1
root root 26288 Aug 5 15:19 browser-webkit.so -rw-r--r-- 1 root root 12200 Aug 5 15:19 exploit-kit.so -rw-r--r-- 1 root root 22416 Aug 5 15:19 file-executable.so -rw-r--r-- 1 root root 8416 Aug 5 15:19 file-flash.so -rw-r--r-- 1 root root 228896 Aug 5 15:19 file-image.so -rw-r--r-- 1 root root 8088 Aug 5 15:19 file-java.so -rw-r--r-- 1 root root 99304 Aug 5
15:19 file-multimedia.so -rw-r--r-- 1 root root 133792 Aug 5 15:19 file-office.so -rw-r--r-- 1 root root 411464 Aug 5 15:19 file-other.so -rw-r--r-- 1 root root 149448 Aug 5 15:19 file-pdf.so -rw-r--r-- 1 root root 18520 Aug 5 15:19 indicator-shellcode.so -rw-r--r-- 1 root root 28440 Aug 5 15:19 malware-cnc.so -rw-r--r-- 1 root root 12208 Aug 5 15:19 malware-
other.so -rw-r--r-- 1 root root 28424 Aug 5 15:19 netbios.so -rw-r--r-- 1 root root 13128 Aug 5 15:19 os-linux.so -rw-r--r-- 1 root root 64320 Aug 5 15:19 os-other.so -rw-r--r-- 1 root root 54880 Aug 5 15:19 os-windows.so -rw-r--r-- 1 root root 144328 Aug 5 15:19 policy-other.so -rw-r--r-- 1 root root 8528 Aug 5 15:19 policy-social.so -rw-r--r-- 1 root root
39256 Aug 5 15:19 protocol-dns.so -rw-r--r-- 1 root root 31216 Aug 5 15:19 protocol-other.so -rw-r--r-- 1 root root 54792 Aug 5 15:19 protocol-scada.so -rw-r--r-- 1 root root 37224 Aug 5 15:19 protocol-snmp.so -rw-r--r-- 1 root root 17256 Aug 5 15:19 protocol-tftp.so -rw-r--r-- 1 root root 49856 Aug 5 15:19 protocol-voip.so -rw-r--r-- 1 root root 8560 Aug
5 15:19 server-iis.so -rw-r--r-- 1 root root 14288 Aug 5 15:19 server-mail.so -rw-r--r-- 1 root root 8000 Aug 5 15:19 server-mysql.so -rw-r--r-- 1 root root 13176 Aug 5 15:19 server-oracle.so -rw-r--r-- 1 root root 268072 Aug 5 15:19 server-other.so -rw-r--r-- 1 root root 883096 Aug 5 15:19 server-webapp.so errors: Loading /opt/snort/etc/rules/snort-
pulledpork.rules: ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:19 SO rule 38758 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:20 SO rule 28487 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:21 SO rule 28488 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:22 SO rule 35721 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:23 SO rule 35722 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:24 SO rule 36218 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:25 SO rule 36219 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:26 SO rule 36220 not loaded. ERROR: /opt/snort/etc/rules/snort-
pulledpork.rules:27 SO rule 36221 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:28 SO rule 51369 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:29 SO rule 53257 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:30 SO rule 53258 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:31 SO
rule 53686 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:32 SO rule 38671 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:33 SO rule 38672 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:34 SO rule 48691 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:35 SO rule 48692 not loaded.
ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:36 SO rule 49912 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:37 SO rule 56059 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:38 SO rule 56060 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:39 SO rule 30282 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:40 SO rule 30283 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:41 SO rule 31398 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:42 SO rule 31451 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:43 SO rule 39379 not loaded. ERROR: /opt/snort/etc/rules/snort-
pulledpork.rules:44 SO rule 30902 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:45 SO rule 30903 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:46 SO rule 30912 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:47 SO rule 30913 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:48 SO
rule 30921 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:49 SO rule 30922 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:50 SO rule 30942 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:51 SO rule 30943 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:52 SO rule 35727 not loaded.
ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:53 SO rule 35728 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:54 SO rule 40299 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:55 SO rule 40300 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:56 SO rule 40767 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:57 SO rule 40768 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:58 SO rule 40769 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:59 SO rule 40770 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:60 SO rule 45524 not loaded. ERROR: /opt/snort/etc/rules/snort-
pulledpork.rules:61 SO rule 45525 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:62 SO rule 46003 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:63 SO rule 46004 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:64 SO rule 46005 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:65 SO
rule 46006 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:66 SO rule 46007 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:67 SO rule 46008 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:68 SO rule 46009 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:69 SO rule 46010 not loaded.
ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:70 SO rule 46011 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:71 SO rule 46012 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:72 SO rule 46013 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:73 SO rule 46014 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:74 SO rule 46015 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:75 SO rule 46016 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:76 SO rule 46017 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:77 SO rule 46018 not loaded. ERROR: /opt/snort/etc/rules/snort-
pulledpork.rules:78 SO rule 46019 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:79 SO rule 46020 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:80 SO rule 46021 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:81 SO rule 46022 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:82 SO
rule 47363 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:83 SO rule 47364 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:84 SO rule 47394 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:85 SO rule 47395 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:86 SO rule 47878 not loaded.
ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:87 SO rule 47879 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:88 SO rule 48689 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:89 SO rule 48690 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:90 SO rule 45597 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:91 SO rule 54028 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:92 SO rule 39885 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:93 SO rule 43424 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:94 SO rule 43425 not loaded. ERROR: /opt/snort/etc/rules/snort-
pulledpork.rules:95 SO rule 43426 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:96 SO rule 43427 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:97 SO rule 43428 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:98 SO rule 43429 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:99 SO
rule 43430 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:100 SO rule 43431 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:101 SO rule 43432 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:102 SO rule 30887 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:103 SO rule 30888 not
loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:104 SO rule 30929 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:105 SO rule 30931 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:106 SO rule 30933 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:107 SO rule 31361 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:108 SO rule 35894 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:109 SO rule 35897 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:110 SO rule 35898 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:111 SO rule 35899 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:112 SO rule 35900 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:113 SO rule 35901 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:114 SO rule 35902 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:115 SO rule 35903 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:116 SO rule 35906 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:117 SO rule 35908 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:118 SO rule 36153 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:119 SO rule 40006 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:120 SO rule 40049 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:121 SO rule 40287 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:122 SO rule 40499 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:123 SO rule 41548 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:124 SO rule 41909 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:125 SO rule 41910 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:126 SO rule 43489 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:127 SO rule 43558 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:128 SO rule 43559 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:129 SO rule 44071 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:130 SO rule 44189 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:131 SO rule 45575 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:132 SO rule 45596 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:133 SO rule 46110 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:134 SO rule 47234 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:135 SO rule 47684 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:136 SO rule 47707 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:137 SO rule 49334 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:138 SO rule 49335 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:139 SO rule 53668 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:140 SO rule 57115 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:141 SO rule 57116 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:142 SO rule 57117 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:143 SO rule 57118 not loaded. ERROR:
```

```
/opt/snort/etc/rules/snort-pulledpork.rules:144 SO rule 52020 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:145 SO rule 52021 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:146 SO rule 49293 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:147 SO rule 57136 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:148 SO rule 35885 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:149 SO rule 44012 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:150 SO rule 38745 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:151 SO rule 56552 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:152 SO rule 56553 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:153 SO rule 49442 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:154 SO rule 49443 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:155 SO rule 35834 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:156 SO rule 35835 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:157 SO rule 16343 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:158 SO rule 41360 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:159 SO rule 41361 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:160 SO rule 41362 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:161 SO rule 41363 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:162 SO rule 42313 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:163 SO rule 42314 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:164 SO rule 45521 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:165 SO rule 45522 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:166 SO rule 45715 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:167 SO rule 45716 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:168 SO rule 46292 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:169 SO rule 46293 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:170 SO rule 46550 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:171 SO rule 46551 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:172 SO rule 47340 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:173 SO rule 47341 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:174 SO rule 49189 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:175 SO rule 49190 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:176 SO rule 38244 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:177 SO rule 38245 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:178 SO rule 38285 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:179 SO rule 38746 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:180 SO rule 38747 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:181 SO rule 38748 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:182 SO rule 38749 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:183 SO rule 38750 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:184 SO rule 38751 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:185 SO rule 38752 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:186 SO rule 38753 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:187 SO rule 38754 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:188 SO rule 38755 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:189 SO rule 38756 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:190 SO rule 38757 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:191 SO rule 57422 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:192 SO rule 31615 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:193 SO rule 31616 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:194 SO rule 34180 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:195 SO rule 47595 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:196 SO rule 47596 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:197 SO rule 47597 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:198 SO rule 47598 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:199 SO rule 34369 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:200 SO rule 35347 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:201 SO rule 35926 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:202 SO rule 35927 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:203 SO rule 35929 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:204 SO rule 35930 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:205 SO rule 35931 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:206 SO rule 35932 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:207 SO rule 35941 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:208 SO rule 36913 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:209 SO rule 37358 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:210 SO rule 38543 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:211 SO rule 39897 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:212 SO rule 40240 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:213 SO rule 40275 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:214 SO rule 41538 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:215 SO rule 45870 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:216 SO rule 46740 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:217 SO rule 46741 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:218 SO rule 46992 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:219 SO rule 47679 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:220 SO rule 47680 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:221 SO rule 47681 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:222 SO rule 48946 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:223 SO rule 48947 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:224 SO rule 48948 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:225 SO rule 48949 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:226 SO rule 49350 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:227 SO rule 49362 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:228 SO rule 49509 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:229 SO rule 49510 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:230 SO rule 49511 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:231 SO rule 49614 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:232 SO rule 49615 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:233 SO rule 49616 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:234 SO rule 49619 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:235 SO rule 50512 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:236 SO rule 50513 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:237 SO rule 50514 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:238 SO rule 50515 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:239 SO rule 50745 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:240 SO rule 51355 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:241 SO rule 52627 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:242 SO rule 52628 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:243 SO rule 52629 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:244 SO rule 52630 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:245 SO rule 52631 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:246 SO rule 52632 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:247 SO rule 53168 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:248 SO rule 53671 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:249 SO rule 53672 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:250 SO rule 53673 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:251 SO rule 53674 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:252 SO rule 53675 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:253 SO rule 53676 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:254 SO rule 53677 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:255 SO rule 53678 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:256 SO rule 53679 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:257 SO rule 53680 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:258 SO rule 53681 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:259 SO rule 53851 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:260 SO rule 54598 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:261 SO rule 54599 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:262 SO rule 54600 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:263 SO rule 54601 not loaded. ERROR:
/opt/snort/etc/rules/snort-pulledpork.rules:264 SO rule 56306 not loaded. ERROR: /opt/snort/etc/rules/snort-pulledpork.rules:265 SO rule 57486 not loaded.
```

19 through 265 in the snort-pulledpork.rules are all the soid rules. There is currently no documentation for a rule with the id 3-49619 There is currently no documentation for a rule with the id 3-49619 There is currently no documentation for a rule with the id 3-49619 There is currently no documentation for a rule with the id 3-49619 To help cybersecurity, networking, and information technology professionals learn Snort 3 fast, we've created the Snort 3 QuickStart Pro. This book offers practical and easy-to-learn coverage into deploying and managing Snort in a variety of network environments to effectively use Snort's powerful intrusion detection and prevention features.The book begins with an introduction to Snort's architecture and configuration, then walks you through setting up Snort for various network scenarios. You will discover how to enhance detection capabilities by writing and implementing Snort rules, using preprocessors, and integrating dynamic modules. You will apply Snort to real-world network problems with the help of examples and detailed instructions. It further teaches performance tuning and optimization strategies, allowing you to handle high traffic loads while maximizing resource efficiency.The book later explains how to set up high availability settings, including redundancy and failover mechanisms, to ensure continuous protection. In addition, a strong emphasis is placed on troubleshooting, with sections dedicated to diagnosing and resolving common issues encountered during Snort deployment and operation. You will learn to analyze logs, debug rules, and optimize configurations for maximum performance and accuracy.Upon completion, you will be able to deploy Snort 3, manage its operations, and adapt it to changing security needs. Equipped with clear explanations and hands-on exercises, this book enables you to improve your network security skills and respond effectively to cyber threats.Key LearningsUp and running with setting up Snort 3 for a wide range of network types and security requirements.Write effective Snort rules to safeguard your network and identify threats with pinpoint accuracy.Maximize Snort's detection capabilities by utilizing preprocessors and dynamic modules.Improve performance and deal with heavy traffic loads by learning Snort's architecture.Setup failover and high availability measures.Check and fix frequent issues to keep Snort running smoothly and reliably.Use Snort's alerting and logging capabilities to oversee and manage network infrastructure.Combine Snort with additional tools for an integrated approach to network security administration.Table of ContentGetting Started with IDPSInstalling and Configuring Snort 3Up and Running with Snort Architecture and OperationsWriting Snort RulesWorking with Preprocessors and Event ProcessingLeveraging Dynamic Modules and PluginsDeploying Snort in a Production Environment Einleitung Dieses Dokument beschreibt die Regeln für die Snort3 Engine in Cisco Secure Firewall Threat Defense (FTD). Voraussetzungen Anforderungen Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen: Cisco Secure Firewall Threat Defense (FTD) Intrusion Prevention System (IPS) Snort2 Syntax Lizenzierung Keine spezifischen Lizenzanforderungen, die Basislizenz ist ausreichend und die genannten Funktionen sind in der Snort-Engine innerhalb der FTD und in den Snort3 Open-Source-Versionen enthalten. Verwendete Komponenten Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen: Cisco Secure Firewall Threat Defense (FTD), Cisco Secure Firewall Management Center (FMC) Version 7.0+ mit Snort3. Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen. Hintergrundinformationen Snort ist die Cisco IPS-Engine, die Datenverkehrsanalysen und Paketprotokollierung in Echtzeit ermöglicht. Snort kann Protokollanalysen durchführen, Inhalte durchsuchen und Angriffe erkennen. Snort3 ist eine aktualisierte Version des Snort2 IPS mit einer neuen Softwarearchitektur, die Leistung, Erkennung, Skalierbarkeit und Benutzerfreundlichkeit verbessert. Snort3-Regeln Sie verwenden dieses LUA-Format, um das Lesen, Schreiben und Überprüfen der Snort3 Regeln zu erleichtern. Regelaktionen Diese neue Version ändert die Regelaktionen. Die neuen Definitionen lauten wie folgt: Pass: Beenden der Auswertung nachfolgender Regeln für Pakete Alert: Nur Ereignis generieren Block: Paket verwerfen, Restsitzung blockieren Drop: Nur Paket verwerfen Rewrite: Erforderlich, wenn die Option replace verwendet wird React: Antwortseite für HTML-Block senden Reject: Injizieren von TCP-RST oder ICMP nicht erreichbar Regelanatomie Die Anatomie ist: Der Regelheader enthält die Aktion, das Protokoll, das Quell- und das Zielnetzwerk sowie die Ports. In Snort3kann der Regelkopf eine der folgenden Optionen sein: