Threat Detection

Cisco's portscan detector is a threat detection mechanism designed to help you detect and prevent portscan activity in all types of traffic to protect networks from eventual attacks. Portscan traffic can be detected efficiently in both allowed and denied traffic.

Portscan is a form of network reconnaissance that is often used by attackers as a prelude to an attack. In a portscan, an attacker determines the types of network protocols or services a host supports and sends specially crafted packets to a targeted host. By examining the packets that the host responds with, the attacker can often determine which ports are open on the host and, either directly or by inference, which application protocols are running on these ports.

Note The portscan detection and prevention feature from the access control policy is supported from management center 7.2 onwards in Snort 3 devices only. Threat detection is eligible for the traffic inspected by Snort only. Threat detection is not considered for traffic sent to the threat defense device itself.

Portscan Detection and Prevention

Types of Detection

The following are the types of portscan activities that can block hosts detecting them.

- **Regular portscan**—A one-to-one portscan in which an attacker uses a host to scan multiple ports on a single target host. This option detects TCP, UDP, and IP portscans.
- **Decoy portscan**—A one-to-one portscan in which the attacker mixes spoofed source IP addresses with the actual scanning IP address. The decoy portscan option detects TCP, UDP, and IP protocol portscans.

- **Distributed portscan**—A many-to-one portscan in which multiple hosts query a single host for open ports. This is used to evade port scan detection as all the requests when sourced from multiple hosts might look legitimate. The distributed portscan option detects TCP, UDP, and IP protocol portscans.
- **Port sweep**—A one-to-many portsweep in which an attacker uses one or a few hosts to scan a single port on multiple target hosts. This usually happens for new exploits and the attacker is looking for a specific service. This option detects TCP, UDP, ICMP, and IP portsweeps.

Note Regular, decoy, and distributed portscans are not categorized and alerted as regular portscan activity.

Traffic Selection

- You can choose portscan detection for **Permitted**, **Denied**, or **All** traffic. By default, portscan detection occurs for all the traffic in a selected category.
- You can specify the networks to be monitored for portscan activity. Within the monitored network, you can exempt certain hosts from being identified as scanners.
- You can also exempt all traffic that is designed to target hosts from portscan detection.
- Portscan detection is supported for both IPv4 and IPv6 traffic.

Detection Configuration

The following are the detection configuration options:

- Configuration options:
  - Protocol types: TCP, UDP, IP, and ICMP
  - Port count: Number of ports accessed for TCP and UDP based scans
  - Host count: Number of hosts accessed for TCP, UDP, and ICMP based scans
  - Protocol count: Number of protocols used for IP protocol scan
  - Interval: Time interval
- Predefined sensitivity levels—You can tune portscan detection using the following sensitivity levels:
  - Low—Detects only negative responses from targeted hosts. Select this sensitivity level to suppress false positives, but remember that some types of portscans (slow scans, filtered scans) might be missed.

    This level uses the shortest time window for portscan detection.
  - Medium—Detects portscans based on the number of connections to a host, so you can detect filtered portscans. However, very active hosts such as network address translators and proxies may generate false positives.

    By default, sensitivity level is set to **Medium**.

    This level uses a longer time window for portscan detection.

- High—Detects portscans based on a time window, which means that you can detect time-based portscans. This level uses a much longer time window for portscan detection.
- Custom—Used to customize sensitivity levels. If you edit existing, preconfigured sensitivity levels, the **Custom** option is automatically selected.

- You can finetune the thresholds and also enable or disable different types of scans.

Prevention Configuration

For configuring prevention, the following are the options:

- You have the option to block a host that has been identified to be performing portscan activity.
- Duration-based block with automatic unblocking of host after duration expires.
- You can exempt hosts from being blocked due to portscan activity.

For more information about configuring portscan detection and prevention, see Configure Portscan Detection and Prevention, on page 3.

Configure Portscan Detection and Prevention

Portscan can be configured either for detection or prevention. By default, portscan detection is done only on allowed traffic.

Before you begin

To configure portscan detection and prevention from the access control policy editor, the following are the prerequisites:

- Management Center and the managed device must be running 7.2.0 or later.
- Snort 3 must be enabled.

Note When you move devices from Snort 3 to Snort 2, portscan gets disabled. However, you can configure portscan on devices using Snort 2 using NAP and intrusion policy.

Procedure

Step 1 In the access control policy editor, click **Advanced Settings** from the **More** drop-down arrow at the end of the packet flow line. Then, click **Edit** (✎) next to **Threat Detection**.

Step 2 In the **Threat Detection** window, you can select **Detection** or **Prevention** as the **Portscan mode**.

Step 3 If you select **Detection**:

a. Under the **Traffic Selection** tab, you have the option to select portscan detection on **Permitted**, **Denied**, or **All** traffic.

b. In the **Monitor**, **Ignore Scanner**, and **Ignore Target** fields, you can select the IPs or networks to consider (monitor) for portscan detection, IPs or networks to be ignored as attackers, and IPs or networks to be ignored as target hosts.

Note FQDN, Wildcard mask, any, any-ipv4, and any-ipv6 network objects are not supported for portscan configuration. These objects are not shown under **Monitor**, **Ignore Scanner**, **Ignore Target**, and **Exclude** fields.

c. Under the **Configuration** tab, you can choose preconfigured sensitivity levels - **Low**, **Medium**, **High**, and **Custom** to tune your postscan detection. Choose the **Custom** option to customize sensitivity levels.

d. Under the different protocol types (TCP, UDP, IP, and ICMP), you can set the number of hosts accessed, number of ports accessed, number of protocols used (for IP protocol), and the interval.

Step 4 You can select the **Prevention** portscan mode to block hosts from further scanning of networks or hosting of an attack. In the **Prevention** tab under **Exclude**, you can choose to exempt IPs or networks from being blocked and also set the **Duration** for blocking the host.

Step 5 To revert portscan settings to default (disabled) state, click the **Revert to Defaults** option.

Step 6 Click **OK** to save the portscan detection and prevention settings.

Step 7 Click **Save** to save the policy.

Note Portscan configuration changes are available as part of AC policy audit log report.

What to do next

Deploy configuration changes; see Deploy Configuration Changes.

Improved Detection in Low Sensitivity

You can track negative responses for TCP, UDP, and ICMP initial packets in low sensitivity levels. Only if the number of unsuccessful connections is more than the rejection threshold (for example, 10% in low sensitivity) and the port/IP protocol count is more than the configured threshold, an alert is triggered. This mitigates false positives.

If there is a mix of allowed and blocked traffic, the number of rejection ports or hosts is calculated based on the difference between allowed and blocked traffic. In the case of only blocked traffic, the rejection threshold is not considered.

Attention This solution does not work for UDP and ICMP connections when threat defense is configured in inline set mode.

Example

Assume the portscan is enabled in threat defense with low sensitivity.

Configured port count threshold = 120

Calculated reject count threshold = 10% of 120 = 12

An attacker initiates the connection with, say, 131 ports of target and the target positively acknowledges all the initiations. Port count = 131, which is greater than the threshold, but an alert is not triggered because there are no negative acknowledgements.

An attacker initiates the connection with, say, 131 ports of target and the target positively acknowledges 121 initiations and negatively acknowledges 10 initiations.

Port count = 131, which is greater than the threshold, but reject port count = 10, which is lesser than the rejection threshold; hence an alert is not triggered.

An attacker initiates the connection with, say, 134 ports of target and the target positively acknowledges 121 initiations and negatively acknowledges 13 initiations. Port count = 134, which is greater than the threshold, reject port count = 13 is also higher than the rejection threshold. Hence an alert is triggered in this case.

Alerting - Portscan Activity

After you configure portscan, the portscan-specific intrusion policy events are generated, regardless of the presence or configuration of IPS policy or events.

Portscan activity is alerted through the existing portscan-specific IPS events. IPS events with Generator ID (GID) 122 and Snort ID from SIDs 1 through 27 are generated. For these events, the *(port_scan)* string is prepended in the event messages.

To view these events in management center, go to **Analysis** > **Intrusion** > **Events**.

Portscan Upgrade from NAP Policy

Snort 3 network analysis policy (NAP)-based portscan feature is not supported on devices running 7.2.0 or later.

For Snort 3 devices running 7.2.0 or later, you must configure portscan using the access control policy (Advanced settings tab).

Post-upgrade to 7.2.0 (or later) Snort 3 device, the portscan configuration settings will be picked and deployed from the access control policy portscan settings instead of the NAP policy, so if you have not migrated your NAP portscan configuration to AC policy portscan, your device will lose the portscan configuration upon next deployment.

The following table shows the portscan configuration that can be applied to version 7.2.0 or later and to version 7.1.0 or earlier that are running Snort 3 or Snort 2 engines.

Management Center	Threat Defense	Portscan Configuration
Management Center 7.0 or 7.1	Snort 2 device	Configuration from Snort 2 NAP Policy is applicable.
	Snort 3 device	Configuration from Snort 3 NAP Policy is applicable.

Management Center	Threat Defense	Portscan Configuration
Management Center 7.2.0	Snort 2 device	Configuration from Snort 2 NAP Policy is applicable.
	Snort 3 device (7.1.0 and earlier)	Configuration from Snort 3 NAP Policy is applicable.
	Snort 3 device (7.2.0 and later)	Configuration from Access Control Policy is applicable.

Feature Support for Access Control Policy with Portscan

Access control policy with portscan is supported for the following features:

- **Audit Logs and Delta Preview**—Portscan information is available in AC policy audit logs and under Deployment Preview.
- **Import and Export**—You can import or export AC policy containing portscan configuration.
- **Domains**—Portscan can be configured for AC policies in global and leaf domains.
- **PDF Report Generation**—The AC policy report also contains the configured portscan settings.
- **Rollback**—You can rollback to the deployed version of the configuration containing the portscan configuration.