|  |  |  |  |
| --- | --- | --- | --- |
| **Type** | Protocol | **Range** | **Purpose of protocol** |
| Custom TCP Rule | TCP | 49152-695535 | Custom TCP Services are **a way for you to create and deploy your own custom services to your Canaries**, without having to write any code. |
| Custom UDP Rule | UDP | 49152-65535 | User Datagram Protocol (UDP) is a communications protocol that is primarily used **to establish low-latency and loss-tolerating connections between applications on the internet**. UDP speeds up transmissions by enabling the transfer of data before an agreement is provided by the receiving party. |
| Custom ICMP Rule-ipv4 | Echo Reply | N/A | ICMP provides **feedback about hosts and networks to the sender of an IP packet**. The routers and switches along the network path are not notified about the errors. An example of ICMP error reporting includes 'host/network not found' when the destination endpoint can't be reached. |
| Custom ICMP Rule -Ipv6 | IPV6 ICMP | All | ICMP in IPv6 functions the same as ICMP in IPv4. ICMP for IPv6 generates error messages, such as ICMP destination unreachable messages, and informational messages, such as ICMP echo request and reply messages. |
| Custom Protocol |  | All | A custom protocol can be assigned the same name as a pre-defined protocol, **in order to extend the number of IP addresses or ports associated with the original protocol**. See Adding to a pre-defined protocol for more information. |
| All TCP | TCP | 0-65535 | The Transmission Control Protocol (TCP) is a transport protocol that is used on top of IP **to ensure reliable transmission of packets**. TCP includes mechanisms to solve many of the problems that arise from packet-based messaging, such as lost packets, out of order packets, duplicate packets, and corrupted packets. |
| All UDP | UDP | 0-65535 | User Datagram Protocol (UDP) – a **communications protocol that facilitates the exchange of messages between computing devices in a network**. It's an alternative to the transmission control protocol (TCP). |
| All ICMP-Ipv4 | ICMP | 0-65535 | It is **used for reporting errors and management queries**. It is a supporting protocol and is used by networks devices like routers for sending error messages and operations information., e.g. the requested service is not available or that a host or router could not be reached |
| All ICMP-Ipv6 | IPV6 ICMP | All | ICMPv6 is an integral part of IPv6 and **performs error reporting and diagnostic functions**. ... Multicast Listener Discovery (MLD) is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like Internet Group Management Protocol (IGMP) is used in IPv4 |
| SSH | TCP | 22 | The SSH protocol (also referred to as Secure Shell) is a **method for secure remote login from one computer to another**. It provides several alternative options for strong authentication, and it protects the communications security and integrity with strong encryption. |
| SMTP | TCP | 25 | The Simple Mail Transfer Protocol (SMTP) is **used to deliver e-mail messages over the Internet**. This protocol is used by most e-mail clients to deliver messages to the server, and is also used by servers to forward messages to their final destination. |
| DNS(UDP) | UDP | 53 | Actually, DNS primarily uses the User Datagram Protocol (UDP) on port number 53 **to serve requests**. DNS queries consist of a single UDP request from the client followed by a single UDP reply from the server. |
| DNS(TCP) | TCP | 53 | DNS uses TCP for **Zone transfer and UDP for name**, and queries either regular (primary) or reverse. UDP can be used to exchange small information whereas TCP must be used to exchange information larger than 512 bytes |
| HTTP | TCP | 80 | (HyperText Transfer Protocol) The communications protocol used to connect to Web servers on the Internet or on a local network (intranet). The primary function of HTTP is **to establish a connection with the server and send HTML pages back to the user's browser**. |
| POP3 | TCP | 110 | Post Office Protocol version 3 (POP3) is a **standard mail protocol used to receive emails from a remote server to a local email client**. POP3 allows you to download email messages on your local computer and read them even when you are offline. |
| IAMP | TCP | 143 | Internet Message Access Protocol (IMAP) is a **protocol for accessing email or bulletin board messages from a (possibly shared) mail server or service**. IMAP allows a client e-mail program to access remote message stores as if they were local. |
| LDAP | TCP | 389 | The Lightweight Directory Access Protocol (LDAP) is a **vendor-neutral application protocol used to maintain distributed directory info in an organized, easy-to-query manner**. That means it allows you to keep a directory of items and information about them. |
| HTTPS | TCP | 443 | HTTPS (Hypertext Transfer Protocol Secure) is an **internet communication protocol that protects the integrity and confidentiality of data between the user's computer and the site**. Users expect a secure and private online experience when using a website. |
| SMB | TCP | 445 | The Server Message Block (SMB) is a network protocol that **enables users to communicate with remote computers and servers — to use their resources or share, open, and edit files**. It's also referred to as the server/client protocol, as the server has a resource that it can share with the client |
| ALL Traffic | All | 0-65535 | IP routing is performed by **all** hosts, as well as routers, whose main **function** is to transport packets across network boundaries. Routers communicate with one. It allows all types of protcols. |
| SMTPS | TCP | 465 | SMTP is **used to transmit e-mail between e-mail servers and from e-mail clients** (such as Microsoft Outlook or UNIX and Linux's sendmail) to e-mail servers (such as Microsoft Exchange). Most e-mail clients, however, use other protocols, such as POP3 or IMAP4, to retrieve e-mail from the server. |
| IMAPS | TCP | 993 | Internet Message Access Protocol (IMAP) is a **protocol for accessing email or bulletin board messages from a (possibly shared) mail server or service**. IMAP allows a client e-mail program to access remote message stores as if they were local. |
| NFS | TCP | 2049 | NFS is an Internet Standard, client/server protocol developed in 1984 by Sun Microsystems to support shared, originally stateless, (file) data access to LAN-attached network storage. As such, NFS **enables a client to view, store, and update files on a remote computer as if they were locally stored** |
| MYSQL/Aurora | TCP | 3306 | o manage instance-level parameters, you **use** DB parameter groups. Each DB instance in an **Aurora MySQL** DB cluster is compatible with the **MySQL** database engine. |
| RDP | TCP | 3389 | Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which **provides a user with a graphical interface to connect to another computer over a network connection**. The user employs RDP client software for this purpose, while the other computer must run RDP server software |
| Redshift | TCP | 5439 | Redshift is a **fast, managed, data warehouse solution** that's part of AWS. ... Redshift uses columnar storage, which means it physically stores the data for each column in contiguous blocks, as opposed to regular transactional databases that store data in rows. This allows it to perform common analysis queries very fast |
| PostgreSQL | TCP | 5432 | PostgreSQL uses a **message-based protocol for communication between frontends and backends (clients and servers)**. The protocol is supported over TCP/IP and also over Unix-domain sockets. |
| Oracle-RDS | TCP | 1521 | Reliable Datagram Socket (RDS) is an open source protocol that is **used for communication over Infiniband**. RDS provides a high-performance and low latency connectionless protocol for communication. It minimizes CPU utilization and is therefore preferred for communication over Infiniband. |
| WinRM-HTTP | TCP | 5985 | The purpose of configuring WinRM for HTTPS is **to encrypt the data being sent across the wire**. WinRM HTTPS requires a local computer Server Authentication certificate with a CN matching the hostname to be installed |
| WinRM-HTTPS | TCP | 5986 | The purpose of configuring WinRM for HTTPS is **to encrypt the data being sent across the wire**. WinRM HTTPS requires a local computer Server Authentication certificate with a CN matching the hostname to be installed. The certificate mustn't be expired, revoked, or self-signed. |
| Elastic Graphics | TCP | 2007 | Amazon Elastic Graphics allows **you to easily attach low-cost graphics acceleration to a wide range of** EC2 instances. Simply choose an instance with the right amount of compute, memory, and storage for your application, and then use Elastic Graphics to add acceleration required by your application. |
| POP3S | TCP | 995 | Post Office Protocol version 3 (POP3) is an **mail protocol used to retrieve mail from a remote server to a local email client**. POP3 copies the mail from the remote server into the local mail client. Optionally, mail is deleted after it is downloaded from the server. This saves space on the server. |
| MY SQL | TCP | 1433 | MySQL Client / Server protocol is **accepted conventions (rules)**. Through these rules client and server “talks” and understand each other. Client connects to server through TCP connection with special socket, sends to server special packets and accepts them from server. |
|  |  |  |  |