Service Objects

Reverse Proxy Service Object (Ingress)

Ingress service objects are used in the ngress/Reverse proxy rules. The object defines a listener port that the Multicloud Defense gateway listens for the traffic it receives and forwards to the target/backend address. Listener port can be configured with a decryption profile that has a TLS certificate configured. When the traffic hits the listener port, Multicloud Defense Gateway returns the TLS certificate configured. consider the following confiugrable options:

- An SNI can be configured on this port. This enables a single listener port (e.g 443) to be proxied to multiple backend targets based on the SNI.
- L7 DoS (L7 Denial of Service) can be configured on the service to set rate limits for an URI and/or HTTP method.
- Target defines the backend address object and port to forward the traffic. The proxied traffic can be forwarded as HTTP, HTTPS, TCP or TLS.

Use the following procedure to create and add a reverse proxy service object:

Step 1 Navigate to **Manage** > **Security Policies** > **Services**.

Step 2 Click **Create**.

Step 3 Click **Reverse Proxy**.

Step 4 Provide a **Name** and **Description**.

Step 5 Configure proxy parameters as defined below:

Option	Description
Decryption Profile	Assign a decryption profile, which also includes the server certificate, to be used for the proxy service.

Option	Description
Dst Port	Assign a destination port. For most web-based services, the destination port will be 443. This is the port Multicloud Defense Gateway listens on for the incoming traffic.
Protocol	TCP is the default.
SNI	Enter the list of SNIs.
L7 DoS	Enter the Layer 7 DoS profile to assign to this proxy service.
Target Backend Port	Enter the Target/Backend application port number.
Protocol	Select the backend protocol.
Address	Select a backend IP address. The IP address in most cases will be the frontend IP of an internal load balancer.

Note If the proxy service is required to run on multiple ports, you can add more entries. However all the ports serve the same certificate and are proxied to the same backend destination address object.

Forward Proxy Service Object (Egress / East-West)

Forward Proxy services are specifically used for HTTP based traffic. The object defines a listener port that the Multicloud Defense Gateway listens for the traffic it receives and forwards to the address/host that's available in the TLS SNI extension header or HTTP Host Header.

Note We recommend using this for egress/east-west traffic.

Use the following procedure to create and add a forward proxy service.

Step 1 Navigate to **Manage** > **Security Policies** > **Services**.
Step 2 Click **Create**.
Step 3 Click **Forward Proxy**.
Step 4 Provide a name and description.
Step 5 Optionally select the Application IDs to match.
Step 6 Configure proxy parameters as defined below.

Option	description
Decryption Profile	Assign a decryption profile, which also includes the certificate. Multicloud Defense impersonates the external certificate by signing it with the certificate provided in this profile. The root certificate is assumed to be installed on all the client application instances.
Dst Port	Assign a destination port. For most web-based services, the destination port will be 443.
Protocol	HTTP or HTTPS.

Note

- Multicloud Defense listens on the **Dst Port** and waits for the HTTP Host header or TLS SNI Header packet. Once Multicloud Defense receives this packet it connects to the host using the protocol. If the protocol is HTTPS, the received certificate data from the external host is signed by the certificate in the decryption profile and sent to the client. The root certificate **must** be installed on the client app instances to avoid a certificate error.
- For a given destination port, there can be only one decryption profile (root CA certificate) association in a policy rule set across all service objects.
- During a forward proxy session, Multicloud Defense Gateway performs a DNS lookup on the destination with DNS request timeout of 30 seconds and cache age-out of TTL seconds.

Forwarding Service Object (Egress / East-West)

Forwarding service objects are used in the forwarding rules. The traffic that matches this type of rule/service is not proxied, and is forwarded as-is. This means there is no deep packet inspection and no Application ID on *encrypted* traffic.

Note We **strongly** recommend using this for East-West traffic.

Use the following procedure to create and add a forwarding service object:

Step 1 Navigate to **Manage** > **Security Policies** > **Services**.

Step 2 Click **Create**.

Step 3 Click **Forwarding**.

Step 4 Provide a name and description.

Step 5 Multicloud Defense supports source NAT on a per service level. For traffic that requires source IP preservation(e.g. East-West traffic), disable SNAT.

For Egress traffic, SNAT **must** always be enabled.

Step 6 Configure port parameters as defined below.

Option	description
Dst Port	Assign a destination port or a range of destination ports as `start-end`.
Protocol	TCP, UDP, ICMP

Note In a forwarding policy, deep packet inspection operations **only** occur on non-encrypted traffic.