Example - Reverse Proxy for Exchange Services

https://campus.barracuda.com/doc/17588/

The reverse proxy redirects incoming requests from Microsoft Exchange Server services to clients without providing the origin details. This example configuration shows how to configure a reverse proxy for the following Microsoft Exchange services:

- Autodiscover
- ActiveSync
- Outlook Web Access
- RPC

The example setup uses the following server and service settings:

Server/Service	Settings
Exchange Server	• FQDN: `mailserver.company.com` • Internal IP Address: `192.168.0.206`
HTTP Proxy Service	• FQDN: No DNS record is available. • External IP Address: `62.99.0.221`
Internal DNS Server	• Internal IP Address: `192.168.0.239`

System Requirements

- Microsoft Exchange Server 2010 SP3

Before You Begin

- Create an HTTP Proxy service on the Barracuda CloudGen Firewall as described in How to Assign Services. Enable the service, choose a descriptive **Service Name** (e.g., RPX), and enter a brief description (e.g., `HTTP Proxy + the location of the customer`).
- Ensure that the matching host access rule allows inbound HTTP/S traffic on port 443. For the inbound host firewall rule named **OP-SRV-PX**, edit the **Service** setting to include **HTTP+S**. For more information on configuring host firewall rules, see Host Firewall.

- For some changes to take effect, it might be necessary to stop and restart the squid process on the Barracuda CloudGen Firewall.
- To prevent DNS issues with internal/external domain resolution, use IP addresses instead of DNS names in the reverse proxy settings.

Step 1. Configure the Proxy Service

Configure the HTTP Proxy service in reverse proxy mode. For reverse proxy to work, virus scanning must be disabled.

Step 1.1 Add the External IP Address of the HTTP Proxy

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > Service Properties**.
2. Click **Lock**.
3. From the **Listening IP** list, select **Explicit**.
4. In the **Explicit IPs** table, add `62.99.0.221`.
5. Click **Send Changes** and **Activate**.

Step 1.2. Configure the Proxy Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. Click **Lock**.
4. Enter the admin proxy email address in the **Contact E-mail** field.
5. In the **Visible Hostname** field, enter the hostname, e.g.: `rpx.company.com`
6. Select **ReverseProxy** as the **Proxy Mode**.
7. In the left menu, select **IP Configuration**.
8. In the **Networking Settings** section, specify the following details:
   - **TCP Listening Port** – Enter 443.
   - **TCP Outgoing Address** – Select **Dynamic**.
   - **UDP Incoming Address** – Select **First-IP**.
   - **UDP Outgoing Address** – Select **First-IP**.
   - **DNS Server IP addresses** – Add `192.168.0.239`.
9. From the **Configuration** menu on the left, select **Malware Protection**.
10. To disable virus scanning, select **No** from the **Enable Virus Scanning** list.
11. Click **Send Changes** and **Activate**.

Step 2. Configure Access Control Settings

Create ACL entries for all Exchange services that must access the Barracuda CloudGen Firewall and for the source IP address range. Then configure the settings for access priority.

In case you have a public FQDN and an official public certificate, you must add the FQDN to **ACL**

Entries and **Domain to backend Mapping**. IP addresses are optional. If you have no FQDN in use, IP addresses are required.

Step 2.1. Configure ACL Entries

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. From the **Configuration Mode** menu, select **Switch to Advanced View**.
3. In the left menu, select **Access Control**.
4. Click **Lock**.
5. From the **Default Access** list, select **Deny**.
6. Create an ACL entry for the Exchange URLs:
    1. In the **ACL Entries** section, click the plus sign (**+**).
    2. Enter a name for the list (e.g., `ExchangeURLs`), select **URL** from the drop down menu and click **OK**.
    3. In the **URL Extensions** table, add the following entries. IP Addresses or FQDNs.
        - `https://62.99.0.221/owa/*`
        - `https://62.99.0.221/rpc/*`
        - `https://62.99.0.221/Autodiscover/*`
        - `https://62.99.0.221/Microsoft-Server-ActiveSync*`
        - `https:// mailserver.company.com/owa/*`
        - `https:// mailserver.company.com/rpc/*`
        - `https:// mailserver.company.com/Autodiscover/*`
        - `https:// mailserver.company.com/Microsoft-Server-ActiveSync*`
    4. Click **OK**.
7. (Optional) Create an ACL entry for URL path extensions:
    1. In the **ACL Entries** section, click the plus sign (**+**).
    2. Enter a name for the list (e.g., `URLPathExtensions`), select **URL Path** from the drop down menu and click **OK**.
    3. In the **URL Path Extensions** table, add values that should be looked up in the URL path following the hostname or IP address. You can add regular expressions, words, or word patterns, e.g.: add the word `example` to look for 'example'
    in http://www.tldomain.com/example/domain/index.html
    4. Click **OK**.
8. Create an ACL entry for the source IP range:
    1. In the **ACL Entries** section, click the plus sign (**+**).
    2. Enter a name for the list (e.g.,`World`), select **Source IP** from the drop down menu and click **OK**.
    3. From the **IP Configuration** list, select **Rangemode**.
    4. In the **IP Ranges** section, enter:
        - **From**: `0.0.0.0`
        - **To**: `255.255.255.255`
    5. Click **OK**.
9. Click **Send Changes** and **Activate**.

Step 2.2. Configure ACL Policies

1. Create an ACL policy to allow the ACL entries that you created.
    1. In the **Access Control Policies** section, click the plus sign (**+**).
    2. Enter a name for the policy (e.g., `ACCE00`) and click **OK**.
    3. In the **ACL Priority** field, enter `10`.
    4. From the **Action** list, select **Allow**.
    5. In the **ACL Entries** section, click the plus sign (**+**)and then select the following entries:
        - **ExchangeURLs**
        - **World**
    6. Click **OK**.
2. Create an ACL policy with a lower priority that denies the **World** ACL entry that you created.
    1. In the **Access Control Policies** section, click the plus sign (**+**).
    2. Enter a name for the policy, (e.g., `ACCE01`) and click **OK**.
    3. In the **ACL Priority** field, enter 99.
    4. From the **Action** list, select **Deny**.
    5. In the **ACL Entries** section, click the plus sign (**+**) and then select **World**.
    6. Click **OK**.
3. Click **Send Changes** and **Activate**.

Step 3. Configure the Reverse Proxy Settings

Enable SSL encryption, specify the back-end web site, and map the addresses of the Exchange services.

Step 3.1. Configure the Reverse Proxy Settings

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > HTTP-Proxy > HTTP Proxy Settings**.
2. In the left menu, select **Reverse Proxy Settings**.
3. From the **Configuration Mode** menu, select **Switch to Advanced View**.
4. Click **Lock**.
5. In the **Backend Web Site** field, enter `62.99.0.221` or the FQDN.
6. From the **Use SSL** list, select **Yes**.
7. In the **SSL Listening port** field, enter 443.
8. Import the **SSL Certificate** and the **SSL Private Key**.
   The certificate must contain the **Name** (`*.company.com`) and **SubAltName** (`DNS:owa.company.com`).
9. In the **Backend IP Addresses** section, click the plus sign (**+**) and then enter `192.168.0.206`.
10. From the **Round Robin** and **Pass Login to Backend** lists, select **No**.

Step 3.2. Configure Domain to Backend Mapping

Map the domains of the Exchange services to the backend web site.

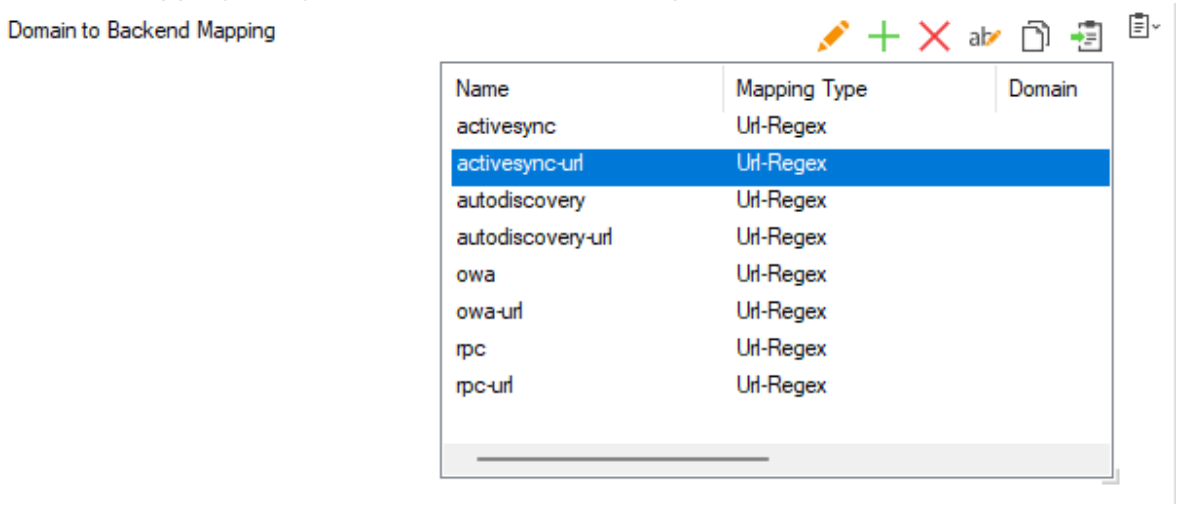
Complete the following steps for each Exchange service:

1. In the **Domain to Backend Mapping** section, click the plus sign (**+**).
2. Enter the name of the Exchange service that you are mapping (e.g., `Autodiscover`) and click **OK**.
3. From the **Mapping Type** list, select **Url-Regex**.
4. In the **Url-Regex** field, enter the domain of the Exchange service that you are mapping:

Exchange Service	Domain
Autodiscover	`https://62.99.0.221/Autodiscover`
ActiveSync	`https://62.99.0.221/Microsoft-Server-ActiveSync`
Outlook Web Access	`https://62.99.0.221/owa`
RPC	`https://62.99.0.221/rpc`

5. From the **Backend** list, select `192.168.0.206` and click **OK**.
6. Click **Send Changes** and **Activate**.

In case you have a public FQDN and an official public certificate, you must configure domain to backend-mapping using FQDNs. IP addresses are optional:



Complete the following steps for each Exchange service:

1. In the **Domain to Backend Mapping** section, click the plus sign (**+**).
2. Enter the name of the Exchange service that you are mapping (e.g., `Autodiscover-URL`) and click **OK**.
3. From the **Mapping Type** list, select **Url-Regex**.
4. In the **Url-Regex** field, enter the domain of the Exchange service that you are mapping:

Exchange Service	Domain
Autodiscover	`https://mailserver.company.com/Autodiscover`
ActiveSync	`https://mailserver.company.com/Microsoft-Server-ActiveSync`
Outlook Web Access	`https://mailserver.company.com/owa`
RPC	`https://mailserver.company.com/rpc`

5. From the **Backend** list, select `192.168.0.206` and click **OK**.
6. Click **Send Changes** and **Activate**.

Figures

1. map_backend.png