Northland DDoS Mitigation

Powered by Corero

Tenant User

USER MANUAL

March 2023

TABLE OF CONTENTS

CLICK ON ANY PAGE NUMBER TO RETURN TO THE TABLE OF CONTENTS

WHAT IS A DDoS ATTACK?

DDoS or "Distributed Denial of Service" is a cyber-attack that targets a specific IP address and attempts to flood a service, website or network with traffic in order to disrupt the service and potentially take it down. The attacker's purpose during this disruption is to navigate your network and attempt to gain access to information while the victim is struggling to figure out what is happening and get their service back up and running.

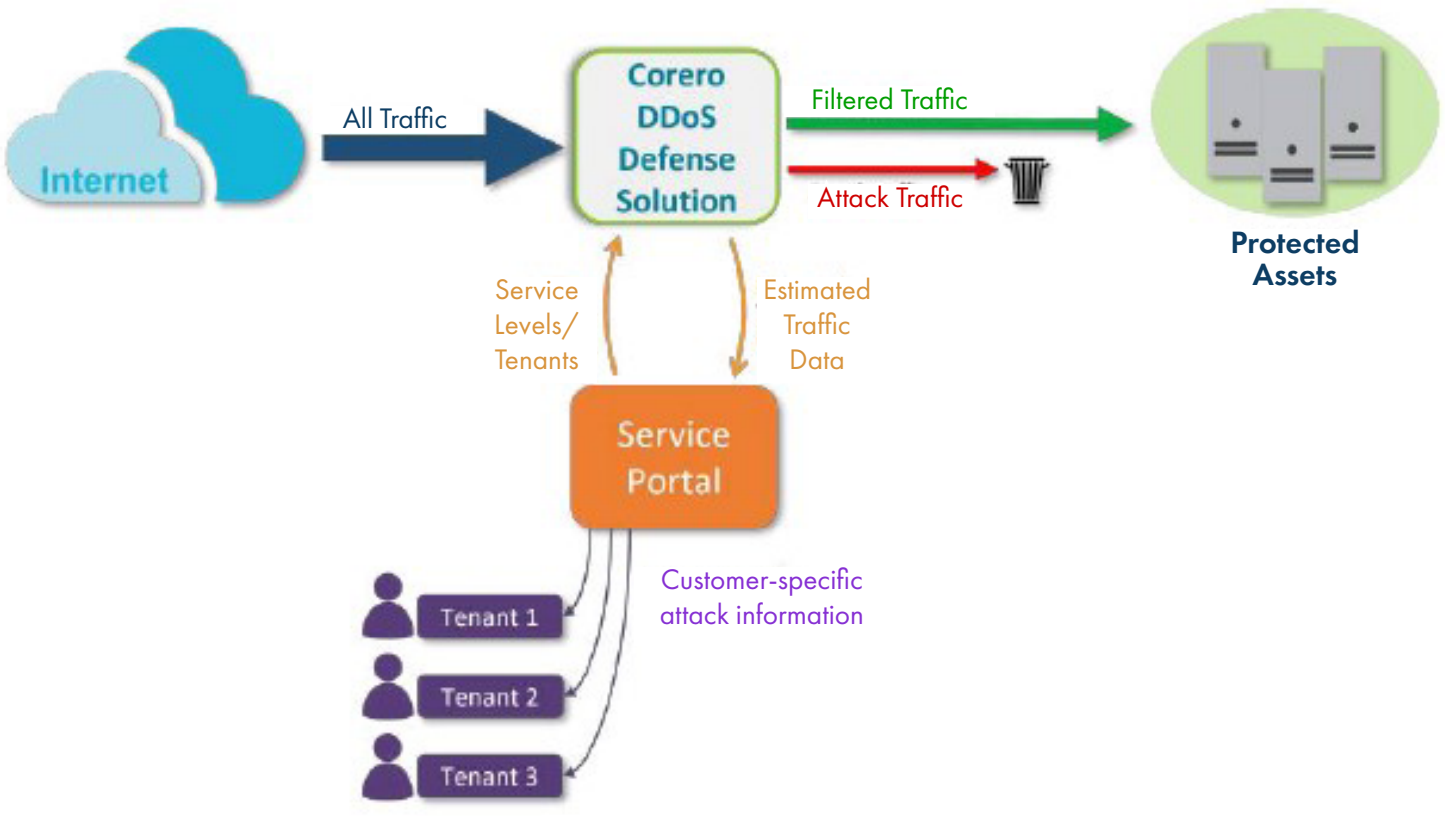
Many attacks are now multi-vector, where attackers combine one or more volumetric, or state exhaustion techniques sequentially, in an attempt to evade detection or mitigation. A volumetric attack overwhelms a network with massive amounts of network traffic to exhaust the target organization's resources. (UDP +ICMP or DNS floodig are examples) This is an ever-evolving threat and therefore an ever-evolving technology

NORTHLAND COMMUNICATIONS DDOS MITIGATION

While Network security is not ever 100% guaranteed, with Northland's DDoS Mitigation Powered by Corero, all traffic is routed through the Corero "SmartWall" appliances in our core network. Good traffic will return to the network while bad traffic is mitigated out. It provides continuous real time monitoring and mitigation from the traffic inbound from our upstream providers.

SMARTWALL SERVICE PORTAL

The SmartWall Service Portal enables you to view and analyze DDoS attacks against your protected assets from a browser. You can use it to understand how many attacks you are being protected from, when they occurred, and what type of attack vector was detected. You can also use the portal to see ongoing attack mitigation, in real time.



WORKING IN THE SERVICE PORTAL

You can access the Service Portal from any of the following supported web browsers:

+ Chrome: 88 or newer
+ Edge: 88 or newer
+ Firefox: 85 or newer
+ Safari: 14 or newer
+ Internet Explorer: not supported

The main navigation is from the main toolbar at the top of each screen. On the left of the main toolbar, you have the portal user functions and, on the right, you have system settings and account options.

Some of the portal screens such as System, also include tabs which enable you to switch between additional views.

Any fields which require input will be indicated inline, with other warnings indicated by a notification panel which appears temporarily in the bottom right corner of the screen, explaining the issue. If everything is working as expected, but there is no data to display in a table or chart, you will see a message such as "No data in this period".

GETTING STARTED

Once you have access to the SmartWall Service Portal you should log in and change your password. Then administrative users can start to configure the Service Portal for your organization.

LOG IN TO THE SERVICE PORTAL

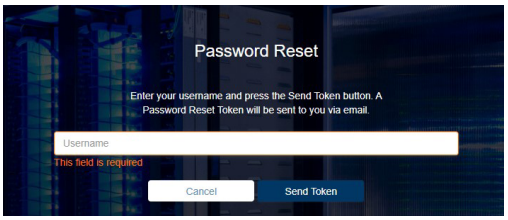
Once you receive login credentials from Northland, you can access the Service Portal via the login page.

IMPORTANT: You are only allowed three failed login attempts before you must reset your password.

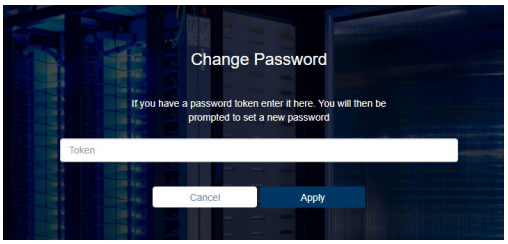
FIRST TIME LOG IN

New tenant users ***do not*** receive a default password. The first time you log into the Service Portal, you will use your email address and the Password Recovery feature to create your password. After that you can log into the Service Portal using your email address and the password you created.
Access the log in screen by entering https://ddos.northland.net

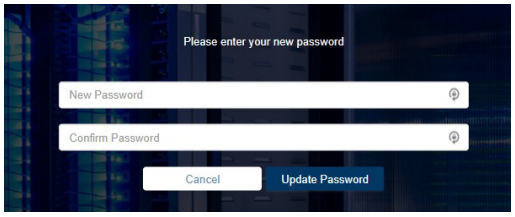
+ At the log in screen, enter your user name (email address).
+ Select **Forgot Password**.
+ In the Token field, enter your **Reset Token**.
+ Select **Apply**.



+ On the Password Reset Screen, enter the email address for your account.
+ Select **Send Token**.
+ When you receive the password reset email it will contain a **Reset Token**.
+ Return to the Service Portal Password Recovery in the browser.



+ In the Token field, enter your **Reset Token**.
+ Select **Apply**.



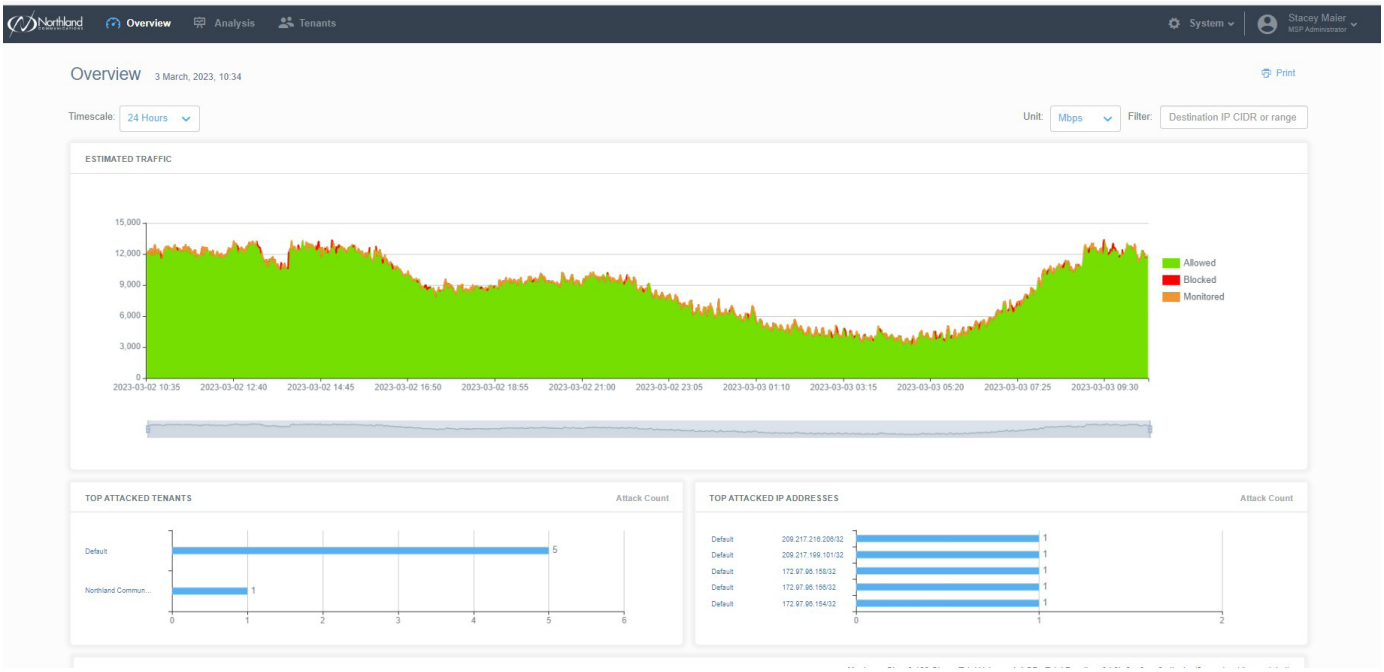
+ Enter your new password in both fields and click **Update Password**.
+ You can now log in to the Service Portal with your new password.

NOTE: A password must be at least 8 characters long; including 1 number, 1 lowercase character, 1 uppercase character and 1 special character from the following list: **$ @ # ! % * ? & ^ - _ ~ . : ( ) { } [ ] ?** .

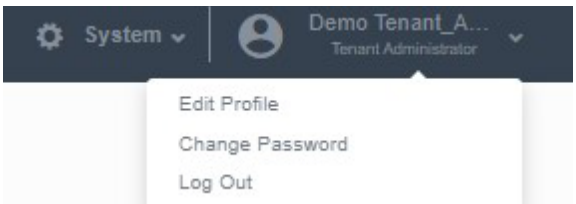
LOG IN TO THE SERVICE PORTAL

+ Go to: https://ddos.northland.net
+ Enter your Username and Password.
+ Select **Log in**.
+ The Service Portal opens on the Service Overview screen.

SAMPLE OVERVIEW SCREEN



LOG OUT OF THE SERVICE PORTAL



+ On the far right of the main toolbar, click your account username.
+ From the drop-down, select **Log Out.**

CHANGE YOUR PASSWORD

When you first access the SmartWall Service Portal, you will be using the default password provided by Northland with you account. You should change this password at the first opportunity. After 180 days, you will be prompted to change your password. If you later forget your password, you can reset it using a **Reset Token** sent to your registered email address.

CHANGE YOUR PASSWORD FROM INSIDE THE SERVICE PORTAL

+ On the right of the main toolbar of the Service Portal, click your **account username**.
+ From the drop-down, select **Change Password**.
+ Enter your Old Password.
+ Enter your new password in both the New Password and Confirm Password fields.
+ Click **Update Password**.
+ The next time you log in, you can use the new password.

RECOVER YOUR PASSWORD USING EMAIL VERIFICATION

If you forget your password, or it expires before you can change it, you can use the **Password Recovery** feature to reset the password in the same way you created the password when you first logged into the Service Portal.

+ At the log in screen, click **Password Recovery**.
+ In the Forgot Password field, enter the email address for your account.
+ Click **Send Email**.
+ When you receive the password reset email it will contain a **Reset Token.**
+ Return to the Service Portal Password Recovery in the browser.
+ In the Token field, enter your **Reset Token**.
+ Click Reset Password.
+ Enter your new password in both fields and click **Update Password**.
+ You can now log in to the Service Portal with your new password.

PASSWORD EXPIRY OPTIONS

For security reasons, all users in the SmartWall Service Portal must reset their password after a period of time. Northland has provisioned this for 180 days.

PASSWORD WARNING AND GRACE PERIODS

When a password expires, the user will no longer be able to log in to the Service Portal. To avoid this, you need to change your password during the warning period or the grace period:

+ **Warning Period (15 days prior to expiration):** During the warning period before the password expires, the user can change their password using the Change Password feature in the Account drop-down or the Password Recovery link on the log in screen.
+ **Grace Period (4 days after the password expires):** During the grace period after the password expires, a user can still change their password using the Password Recovery link on the log in screen. You will not be notified they are in the grace period.

If a user does not change their password during the warning period or grace period, they must contact their administrator to have the password reset.

EDIT YOUR USER PROFILE

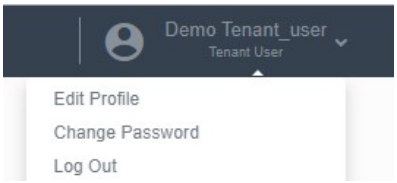
Northland Communications will configure the basic settings for your SmartWall Service Portal by adding the list of assets that are covered by the DDoS protection service, and by creating at least one Tenant Administrator account. A Tenant Administrator, can now further configure those features for your organization:

+ Manage assets
+ Create asset groups
+ Create user accounts for your colleagues

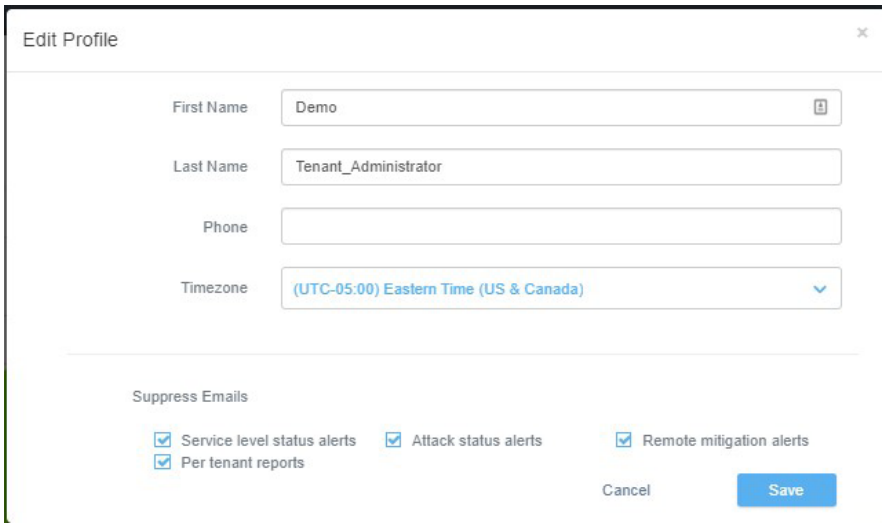
As a Tenant User, you can view attacks and view the asset list, but not make any changes.

Administrators can also edit a user's details.

You can edit some details of your user profile.



+ On the right of the main toolbar of the Service Portal, click your account username.
+ From the drop-down, select **Edit Profile.**



+ You can edit the following details:
  + First Name and Last Name
  + Phone number
  + Timezone
+ You can choose to suppress emails by checking the boxes next to any of the following:
  + Service level status alerts
  + Attack status alerts
  + Service overview reports
  + Per tenant reports
+ When editing is complete, select **Save**.

NOTE: Configuring the Service Portal must be performed by a Tenant Administrator.

SERVICE OVERVIEW AND ATTACK ANALYSIS

You can use the Service Overview and Attack Analysis screens of the SmartWall Service Portal to analyze DDoS attacks which are prevented from impacting your protected assets.

NOTE: The Service Portal is sent traffic data from Northland's DDoS protection platform. If that platform identifies blocked traffic at over 750 pps or 7 Mbps, an attack record is created and sent to the Service Portal. You may still see the blocked traffic from very small attacks on Service Portal traffic graphs, but it is not registered as an attack in the Service Portal. This rate threshold cannot be modified and prevents the Service Portal from sending a large number of attack alert emails for very small attacks.

The Service Overview screen displays information on prevented attacks against all your protected assets. You can change the timescale for this screen and, if your date range includes the current date and time, you can see ongoing attacks.

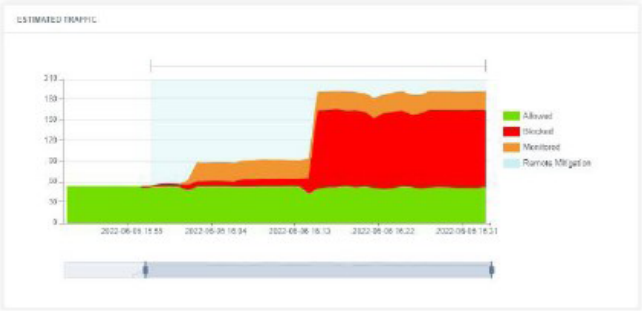
The Attack Analysis screen enables you to search more specifically for attacks and filter those results by date range. For example, if you were looking for an attack that happened yesterday to an asset called Server1, you could select **Asset Name** from the drop-down list and then enter "Server1" into the search field. Then, from the date filters, you could select **24 Hours**. The attack table would now show only attacks in the last 24 hours against an IP address that is associated with Server1.

Each attack has a unique Attack ID which you can use to identify it, when discussing with a provider. In the Attack Analysis screen, you can also expand each attack in the table. This enables you to see a chart of its traffic profile, where you can use the sliders to focus in on the blocked and allowed traffic for specific times during that attack.

NOTE: You can click on a piece of information in a chart in the Overview screen, and the Attack Analysis screen will open showing the data point you clicked in the Overview chart.

TRAFFIC CHARTS

On the Service Overview and Attack Analysis screens, you can see charts displaying your estimated traffic rate.



The total estimated traffic rate is shown by the height of the graph in either Megabit Per Second (Mbps) or Packets Per Second (PPS) depending on the **Units** filter you have selected for this screen. Within the total rate, it is broken down by how the traffic has been handled:

+ **Green:** Non-attack traffic which has been **allowed** to continue to your protected assets.
+ **Red:** Potential attack traffic which has been **blocked** from reaching your protected assets.
+ **Orange:** Potential attach traffic which has not been blocked. The traffic is being monitored but is still allowed to continue to your protected assets. This may be due to the Service Level you currently subscribe to.

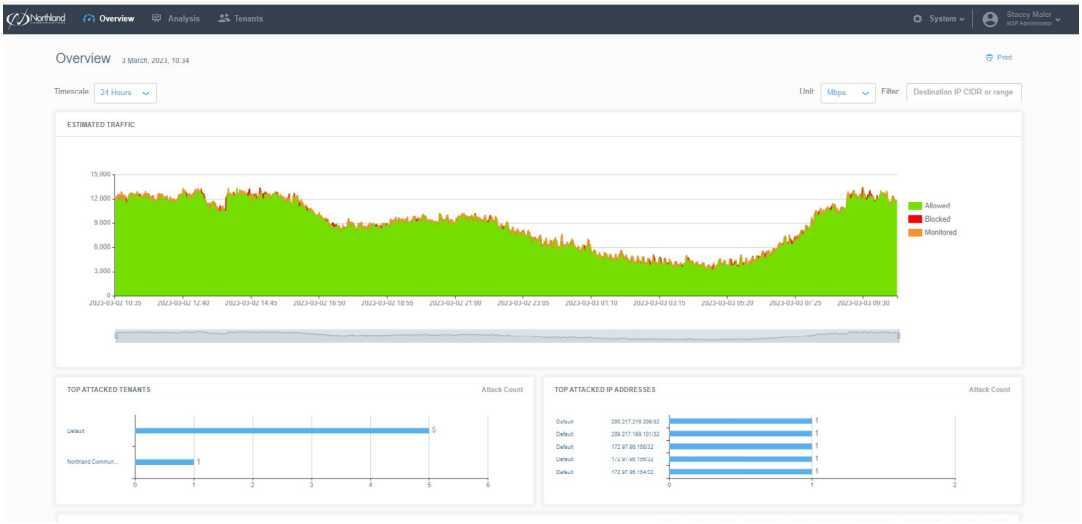
When Northland has **Remote Mitigation** display enabled, you may see some time periods shaded **light blue**. This indicates that an upstream Remote Mitigation may be affecting your traffic during this time period.

PRINT ATTACK REPORTS

In the top right corner of the Service Overview and Attack Analysis screens there is the print button. This enables you to print a report from the information you are currently looking at. On the Service Overview screen this button prints the charts and attack table for the current date range you have selected. On the Attack Analysis screen this button prints the attacks table filtered by the date filter you have selected, and the results of any search entered in the Search bar.

SERVICE OVERVIEW SCREEN

You can navigate to the Service Overview screen by clicking **Overview** on the main toolbar.



FILTERS

The date filters at the top of the Service Overview screen change the charts and table below to show only data for that timescale. You can click Timescale to select from a list of date filters:

+ **Last Hour:** Only data from the last hour.
+ **24 Hours:** Only data from the last 24 hours.
+ **7 Days:** Only data from the last 7 days.
+ **30 Days:** Only data from the last 30 days.
+ **Custom:** Use the date/time fields to set a start date and time in the first field then an end date and time in the second field. The charts and table below then show only data from that time period.

The Unit filter enables you to display traffic rates in Megabits Per Second (Mbps) or Packet Per Second (PPS).

The Destination IP CIDR or range Filter, at the top right of the screen, can be used to show only the specified DIP, CIDR, or range on the charts.

The filters affect all charts and tables on the Service Overview screen. See Charts and Tables.

CHARTS AND TABLES

ESTIMATED TRAFFIC CHART: Displays the sampled allowed inbound traffic and sampled blocked traffic (in megabits per second) for your protected assets, over the selected time period.
The green area on the chart denotes allowed traffic and the red area denotes blocked traffic. You can hover over the areas to see exact values of allowed or blocked traffic. You can also hide/show a type of traffic by clicking on **Allowed Traffic** or **Blocked Traffic** in the top right of the chart.
To focus on a specific section of the time period you can use the sliders on the smaller line chart below the main display. Slide them in to focus on a particular time frame and slide them out to view the entire time period again.

TOP ATTACKED IP ADDRESSES CHART: Displays the 5 IP addresses that received the most attacks during the selected time period. The exact number of attacks is displayed at the end of each bar.

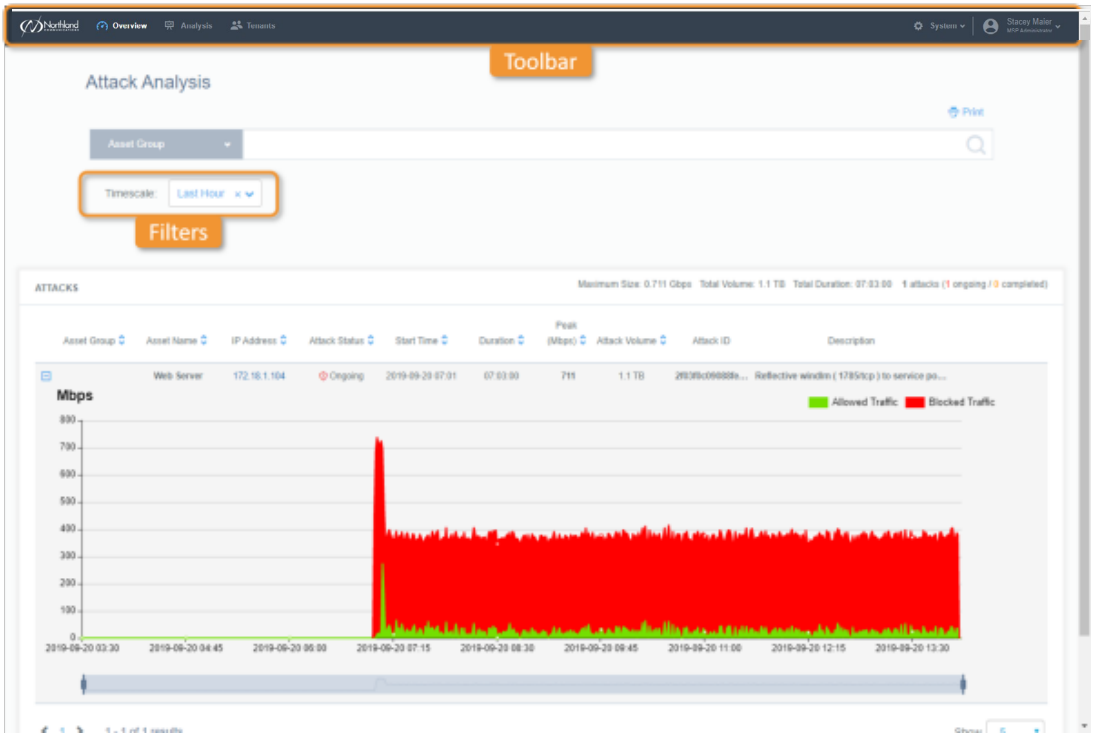
ATTACKS TABLE: Displays every attack on your assets during the selected time period. In the top right corner, you can see the total number of attacks broken down into **ongoing** and **completed**.
At the top of the Attacks table, you can view a summary of the current table content. This shows the **Maximum Size** of attacks, **Total Volume** of all attacks, **Total Duration** of the attack period shown in the table, and the number of attacks listed broken down into **ongoing** and **completed**.

The Attacks table displays the following information for each attack:
+ **Asset Name:** If the IP address is part of a named asset this is displayed here. Otherwise this field is blank.
+ **IP Address:** The IP address which is the target of the attack. Click to view all attacks against this IP address.
+ **Attack Status:** An attack can be **Ongoing** or **Completed**.
+ **Start Time:** The time that the attack traffic was first detected.
+ **Duration:** For an ongoing attack, this is the amount of time since the attack started. For a completed attack, this is the total amount of time attack traffic was detected . The time is shown in the format hh:mm:ss (e.g. 02:10:00 describes an attack lasting 2 hours and 10 minutes).
+ **Peak (Mbps):** For an ongoing attack, this field shows the current peak value. For a completed attack it shows the highest rate of attack traffic detected during the attack in megabits per second (mbps).
+ **Attack Volume:** The volume of traffic sent over the duration of this attack. Only available for SWA 9.7.0 and later, other versions show **n/a**.
+ **Description:** A summary of the attack characteristics. If the description is truncated, hover over it to see the full text.

You can click **Print** in the top right to print the selected view or save it in PDF format.

ATTACK ANALYSIS SCREEN

You can navigate to the Attack Analysis screen by clicking Analysis on the main toolbar.



The **Search** bar and drop-down at the top of the Attack Analysis screen enables you to search for specific attacks. You can select one of the following categories and type a search term:

+ **Attack ID:** If you type a full Attack ID, the Attacks table only shows attacks made against that Attack ID. If you type a partial Attack ID, the Attacks table shows all results that include the search term in the Attack ID field.
+ **Asset Name:** The Attacks table only shows results that include the search term in the Asset Name field.
+ **Asset Group:** The Attacks table only shows results that include the search term in the name of the Asset Group.

Just like the Service Overview screen you can also use the date filters to change the time period for which the table shows data. You can use the filter and search individually or together to narrow down the results in the Attacks table.

The Attacks table displays every attack that matches the search term, and which occurred during the selected time period. In the top right corner, you can see the total number of attacks broken down into ongoing and completed. You can re-order the table using the column headers.

At the top of the Attacks table, you can view a summary of the current table content. This shows the **Maximum Size** of attacks, **Total Volume** of all attacks, **Total Duration** of the attack period shown in the table, and the number of **attacks** listed broken down into **ongoing** and **completed**.

ATTACKS TABLE

The Attacks table displays every attack tht matches the search term and which occured during the selected time period. In the top right corner you can see the total number of attacks broken down into ongoing and completed. You can re-order the table using the column headers and refresh the table to get the latest information using the refresh icon next to the table title.

At the top of the Attacks table, you can view a summary of the current table content. This shows the **Maximum Size** of attacks, **Total Volume** of all attacks, **Total Duration** of the attack period shown in the table, and the **number of attacks** listed broken down into **ongoing** and **completed**.

The Attacks table displays the following information for each attack:

+ **Expand:** Click the expand icon to view a Traffic chart for the period of the selected attack. The green area on the chart denotes estimated allowed traffic and the red area denotes estimated blocked traffic. You can hover over the areas to see values of allowed or blocked traffic. You can also hide/show a type of traffic by clicking on **Allowed Traffic** or **Blocked Traffic** in the top right of the chart.
  To focus on a specific section of the time period you can use the sliders on the smaller line chart below the main display. Slide them in to focus on a particular time frame and slide them out to view the entire time period again. The timeline has 50% of the total attack time either side of the attack to show it in context.

+ **Asset Name:** If the IP address is part of a named asset (in the tenant's asset list) this is displayed here. Otherwise this field is blank.
+ **IP Address:** The IP address which is the target of the attack.
+ **Attack Status:** An attack can be **Ongoing** or **Completed**.
+ **Start Time:** The time that the attack traffic was first detected .
+ **Duration:** For an ongoing attack, this is the amount of time since the attack started. For a completed attack, this is the total amount of time attack traffic was detected. The time is shown in the format hh:mm:ss (e.g. 02:10:00 describes an attack lasting 2 hours and 10 minutes).
+ **Peak (Mbps):** For an ongoing attack, this field shows the current peak value. For a completed attack it shows the highest rate of attack traffic detected during the attack in megabits per second (Mbps).
+ **Attack Volume:** The volume of traffic sent over the duration of this attack. Only available for SWA 9.7.0 and later, other versions show **n/a**.
+ **Attack ID:** A unique ID which identifies this attack. You can use this when discussing a specific attack with your provider.
+ **Description:** A summary of the attack characteristics. If the description is truncated, hover over it to see the full text.

You can click **Print** in the top right to print the selected view or save it in PDF format.

COMMON ANALYSIS TASKS

On the Service Overview and Attack Analysis screens of the SmartWall Service Portal, you can use the date and search filters to view specific attack data. You can use these tools individually or together to filter the tables and charts to only show the information you need. The following are some of the most common tasks you may want to complete using these tools:

VIEW ANY ONGOING ATTACKS AGAINST YOUR ASSETS

+ From the main toolbar of the Service Portal, click **Overview**.
+ At the **Timescale** drop-down, select **Custom**.
+ Make sure that the second field is showing the current date.
+ Look at the **ATTACKS** table. Click the **Attack Status** column header to reorder the table so that all ongoing attacks are at the top.

VIEW THE MOST ATTACKED IP ADDRESSES IN THE PAST WEEK

+ From the main toolbar of the Service Portal, click **Overview**.
+ From the **Timescale** drop-down select **7 Days**.
+ Look at the **TOP ATTACKED IP ADDRESSES** chart. Here you can see a visualization of the top 5 most attacked IP addresses in your network. You can see the exact number of attacks each experienced at the end of the blue bar.

VIEW ALL ATTACKS AGAINST A SINGLE ASSET

+ From the main toolbar of the Service Portal, click **Analysis**.
+ From the Search drop-down, select **Asset Name**.
+ In the search bar, type the name of the asset whose attacks you want to view.
+ The **ATTACKS** table now shows only the attacks which have that search term in the Asset name column.

VIEW ALL ATTACKS BETWEEN TWO DATES

+ From the main toolbar of the Service Portal, click **Analysis**.
+ At the **Timescale** drop-down, select **Custom**.
+ Click into the first date field. Use the calendar to select the first date. If you want to set a time, click the time at the botttom (e.g. 00:00) and use the arrows to set the hours and minutes. To return to the calendar, click the date at the top (e.g. 01/01/2019).
+ Click into the second date field and repeat the process for the closing date.
+ The **ATTACKS** table now shows only the attacks which have happened between your two selected dates.

VIEW ALL ATTACKS AGAINST AN ASSET IN THE PAST DAY

+ From the main toolbar of the Service Portal, click **Analysis**.
+ From the Search drop-down, select Asset Name.
+ In the search bar, type the name of the asset whose attacks you want to view.
+ From the Timescale drop-down select **24 Hours**.
+ The **ATTACKS** table now shows only the attacks which have happened in the last 24 hours and that contain that search term in the Asset name column.

PRINT A REPORT SHOWING ALL ATTACKS AGAINST AN IP ADDRESS IN THE LAST WEEK

+ From the main toolbar of the Service Portal, click **Analysis.**
+ From the Search drop-down, select **IP Address**.
+ In the search bar, enter the IP address you want to view attacks agains.
+ From the **Timescale** dropdown, select **7 Days.**
+ The **ATTACKS** table now shows only the attacks which have been directed at the IP address over the last week.
+ Click **Print**. Adjust any printer settings you require, then click **Print** again.
+ The report listing all the attacks directed at that IP address over the last week will be printed.