



Monitoring Events

- [Monitoring Events, on page 1](#)

Monitoring Events

After you deploy universal ZTNA, you can monitor the access events in real time. Traffic to and from the private resources that traverses the Firewall Threat Defense is sent to Secure Access. Secure Access aggregates event logs from all access points and provides a centralized monitoring dashboard.

To see a log of the universal ZTNA activities, do these steps:

1. In Security Cloud Control, choose **Secure Access > Monitor > Activity Search**.
2. Click **All** under the **Filters** menu and select **ZTNA Client-based**.

Activity Search

Schedule

Export CSV

LAST 24 HOURS

FILTERS

Search by domain, identity, or URL

Advanced

CLEAR

Saved Searches

Customize Columns

ZTNA Client-based

SAVE SEARCH

ENFORCED BY

FTD

69 Total

Viewing activity from Jun 5, 2025 11:20 AM to Jun 6, 2025 11:20 AM

Page: 1

Results per page: 50

1 - 50

Response

Select All

☐ Allowed

☒ Advanced

☐ Blocked

☐ Blocked PDNS

Enforced By

Select All

☐ Secure Access Cloud

☒ FTD

☐ Umbrella Cloud

Identity Type

Select All

☐ AD Users

☐ AD Groups

☐ AD Devices

☐ SAML Users

Destination	Destination IP	Destination Port	Action	Resource/Application	Rule Name	OS
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi
unifiedfin.acme.com	172.31.76.197	443	Allowed	unifinapp-local	cloudlocalrules	wi

3. Choose **FTD** to monitor the events and policies enforced by the Threat Defense device.

