Introduction to Identity Data

You can configure identity policies to use User Agents, ISE devices, or captive portal to obtain data about the users on your network.

Uses for Identity Data

Collecting identity data allows you to take advantage of many features, including:

- perform user control by writing access control rules using realm, user, user group, and ISE attribute conditions
- alert you via SNMP trap or syslog when the system generates an intrusion event with a specific impact flag

User Detection Fundamentals

You can use your identity policies to monitor user activity on your network, which allows you to correlate threat, endpoint, and network intelligence with user identity information. By linking network behavior, traffic, and events directly to individual users, the system can help you to identify the source of policy breaches, attacks, or network vulnerabilities. For example, you could determine:

- who owns the host targeted by an intrusion event that has a Vulnerable (level 1: red) impact level
- who initiated an internal attack or portscan
- who is attempting unauthorized access of a server that has high host criticality
- who is consuming an unreasonable amount of bandwidth
- who has not applied critical operating system updates
- who is using instant messaging software or peer-to-peer file-sharing applications in violation of company IT policy

Armed with this information, you can use other features of the ASA FirePOWER module to mitigate risk, perform access control, and take action to protect others from disruption. These capabilities also significantly improve audit controls and enhance regulatory compliance.

After you configure user identity sources, you can perform user awareness and user control.

User awareness

The ability to view and analyze user data

User control

The ability to configure user access control rule conditions to block users or user activity in traffic on your network, based on conclusions you drew from user awareness.

You can obtain user data from authoritative identity sources (referenced by your identity policy).

An identity source is authoritative if a trusted server validated the user login. You can use the data obtained from authoritative logins to perform user awareness and user control. Authoritative user logins are obtained from passive and active authentications:

- *Passive authentications* occur when a user authenticates through an external server. The User Agent and ISE are the only passive authentication methods supported by the ASA FirePOWER module.
- *Active authentications* occur when a user authenticates through a Firepower device. Captive portal is the only active authentication method supported by the ASA FirePOWER module.

The following table provides a brief overview of the user identity sources supported by the ASA FirePOWER module.

Table 29-1

User Identity Source	Server Requirements	Source Type	Authentication Type	User Awareness?	User Access Control?	For more information, see...
User Agent	Microsoft Active Directory	authoritative logins	passive	Yes	Yes	The User Agent Identity Source, page 31-2
ISE	Microsoft Active Directory	authoritative logins	passive	Yes	Yes	The Identity Services Engine (ISE) Identity Source, page 31-4
Captive portal	LDAP or Microsoft Active Directory	authoritative logins	active	Yes	Yes	The Captive Portal Identity Source, page 31-6

Consider the following when selecting identity sources to deploy:

- you must use captive portal to record failed authentication activity. A failed authentication attempt does not add a new user to the list of users in the database.
- you must deploy an appliance that has an IP address for its sensing interface (for example, a routed interface) in order to use captive portal.

User Identity Deployments

When the system detects user data from a user login, from any identity source, the user from the login is checked against the list of users in the user database. If the login user matches an existing user, the data from the login is assigned to the user. Logins that do not match existing users cause a new user to be created, unless the login is in SMTP traffic. Non-matching logins in SMTP traffic are discarded.

The User Activity Database

The user activity database on the device contains records of user activity on your network reported by all of your configured identity sources. The system logs events in the following circumstances:

- when it detects individual logins or logoffs
- when it detects a new user
- when you manually delete a user
- when the system detects a user that is not in the database, but cannot add the user because you have reached your user limit

The Users Database

The users database contains a record for each user reported by your configured identity sources.

- The total number of users the device can store depends on the model. When the limit has been reached, you must delete users (manually or with a database purge) to allow new users to be added.

If an identity source is configured to exclude specific user names, user activity data for those user names are not reported to the ASA FirePOWER module. These excluded user names remain in the database, but are not associated with IP addresses.

Current User Identities

When the system detects multiple logins to the same host by different users, the system assumes that only one user is logged into any given host at a time, and that the current user of a host is the last authoritative user login. If multiple users are logged in through remote sessions, the last user reported by the server is the user reported to the ASA FirePOWER module.

When the system detects multiple logins to the same host by the same user, the system records the first time that a user logs into a specific host and disregards subsequent logins. If an individual user is the only person who logs into a specific host, the only login that the system records is the original login.

If another user logs into that host, however, the system records the new login. Then, if the original user logs in again, his or her new login is recorded.

User Database Limits

Your device model determines how many users you can monitor, as well as how many users you can use to perform user control.

Note If your deployment includes an ASA5506-X, ASA5508-X, or ASA5516-X device, you can store a maximum of 2,000 authoritative users.

The ASA FirePOWER User Limit

Your device model determines how many individual users you can monitor. When the system detects activity from a new user, that user is added to the Users database. You can detect users using User Agents, ISE, and captive portal.