

Top 5 Network Device Incidents You Need Visibility Into

Table of Contents

#1: Configuration Changes	3
#2: Repeated Failed Logon Attempts	4
#3: VPN Logon Attempts	5
#4: Hardware Malfunctions	6
#5: Scanning Threats	7
About Netwrix Corporation	8

#1: Configuration Changes

You need to stay on top of all changes to the configuration of your network devices, such as their protocols, ports and connection limits, since any unauthorized or improper modification could lead to connectivity issues — including the entire network becoming unreachable. You also need to know quickly if someone modifies a Group Policy or creates a new user, since that could be a sign of an insider attack or privilege abuse. Netwrix Auditor tracks both successful and failed configuration changes, enabling you to easily answer questions like these:

- ✓ Who erased the configuration of a particular network appliance?
- ✓ What specific settings were changed in the firewall?
- ✓ Which IP address was the reload command initiated from?
- ✓ When was the router password reset?

← Search

WHO
 ACTION
 WHAT
 WHEN
 WHERE

☰ Tools

○ Data source "Network Devices" ×
 ○ Object type "Configuration" × "User" ×
 Action "Modified" × "Removed" × "Added" ×

Open in new window
SEARCH
 Advanced mode

Who	Object type	Action	What	Where	When	Details
John Morales	Configuration	■ Removed	172.28.9.220	172.28.9.220	9/03/2018 9:31:29 AM	Activity record details Data source: Network Devices Monitoring plan: CISCO ASA Visibility Plan Item: 172.28.0.0 – 172.28.254.254 (IP range) Workstation: 1.0.0.15 Details: Action name: Write erase Received from: 172.28.9.220 Priority: 187 Severity: 5 (Notice) Source: ASA Facility: 23 (Local use 7)
Michael Gold	User	■ Modified	Role	172.28.9.220	9/03/2018 9:29:31 AM	
Michael Gold	User	■ Added	John Morales	172.28.9.220	9/3/2018 9:01:08 AM	

#2: Repeated Failed Logon Attempts

It is critical to monitor successful logons to network devices to make sure that they are fully authorized. However, you also need to watch for multiple failed logon attempts, which could indicate that someone is trying to brute-force administrative credentials. If attackers get access to your network device, they'll be able to gain control over your network traffic and steal sensitive data. Netwrix Auditor tracks both successful and failed logon attempts, helping you promptly detect potential brute-force attacks and quickly answer questions like these:

- ✓ Who exceeded the maximum number of consecutive authentication failures?
- ✓ What was the cause of each failed logon?
- ✓ Which IP address was the connection made from?
- ✓ How many logons were attempted?
- ✓ When was each failed authentication request made?
- ✓ What device was the user trying to log on to?

The screenshot shows a search interface with filters for Data source: "Network Devices", Object type: "Logon", and Action: "Failed logon". The results table shows three entries for user Mitch Anderson, all with the action "Failed Logon" and workstation "1.2.0.10". The details pane on the right shows activity record details for the first entry.

Who	Object type	Action	What	Where	When	Details
Mitch Anderson	Logon	Failed Logon	management: 66.249.79.96/https	66.249.79.96	9/07/2018 1:01:17 PM	Activity record details Data source: Network Devices Monitoring plan: CISCO ASA Visibility Plan Item: 188.243.82.1 – 188.243.82.254 (IP range) Item: 188.243.82.1 – 188.243.82.254 (IP range) Workstation: 1.2.0.10 Details: Action name: Login failed Received from: 66.249.79.9 Priority: 187 Severity: 7 (Notice) Source: ASA Facility: 20 (Local use 4)
Mitch Anderson	Logon	Failed Logon	management: 66.249.79.96/https	66.249.79.96	9/07/2018 01:01:00 AM	
Mitch Anderson	Logon	Failed Logon	management: 66.249.79.96/https	66.249.79.96	9/07/2018 01:00:38 AM	

#3: VPN Logon Attempts

Administrators rarely have to log into network devices remotely, so it is important to keep track of each VPN logon attempt. Moreover, even an authorized device with a secure connection to the corporate network can be hacked and used to gain access to sensitive files. Netwrix Auditor helps you monitor both successful and failed VPN attempts to log on to your network devices and answer questions like the following:

- ✓ Who tried to access network devices over a VPN?
- ✓ Which IP address was the authentication attempt made from?
- ✓ What was the cause of each failed VPN logon?
- ✓ When was each VPN logon attempt initiated?
- ✓ What device was the user attempting to log on to?

The screenshot shows the Netwrix Auditor search interface. At the top, there are filters for WHO (User), ACTION (Logon), WHAT (Authentication), WHEN (Date/Time), and WHERE (IP Address). The search criteria are set to Data source: "Network Devices" and Object type: "Authentication".

Who	Object type	Action	What	Where	When	Details
Nancy Andrews	Authentication	Successful Logon	172.28.9.220	172.28.9.220	9/06/2018 7:11:21 PM	Activity record details Data source: Network Devices Monitoring plan: CISCO IOS Visibility Plan Item: 172.28.0.0 – 172.28.254.254 (IP range) Details: Action name: User authentication succeeded Received from: 172.28.9.220 Priority: 189 Severity: 5 (Notice) Parser name: Cisco IOS: VPN logons Facility: 23 (Local use 7) Destination: 44.55.67.88
Nancy Andrews	Authentication	Failed Logon	Internal: 172.19.36.85/ssh	172.28.9.220	9/06/2018 7:11:00 AM	
Nancy Andrews	Authentication	Successful Logon	172.15.4.110	172.15.4.110	9/06/2018 07:10:15 AM	

Additional details for the first entry (Successful Logon):
 Action name: User authentication succeeded

#4: Hardware Malfunctions

In addition to tracking changes to the configuration of your network devices, you should also keep a close eye on the state of your hardware. If a network device encounters environmental or power conditions that violate its specifications, it can overheat, suffer ventilation failures or lose power, which lead to underperformance or even complete shutdown of your network. Network Auditor monitors and alerts on critical hardware failures and helps you answer questions like these:

- ✓ What actions happened before the network device shutdown?
- ✓ Which part of the network device got damaged?
- ✓ When did the temperature reach critical level?

← Search
WHO
ACTION
WHAT
WHEN
WHERE
Tools

Data source "Network Devices" ×
Object type "RAM" × "CPU" × "Environment" ×
Action "Modified" ×

Open in new window
SEARCH
Advanced mode

Who	Object type	Action	What	Where	When	Details
system	CPU	Modified	172.28.9.220	172.28.9.220	9/05/2018 11:31:29 AM	Activity record details Data source: Network Devices Monitoring plan: CISCO ASA Visibility Plan Item: 172.28.0.0 – 172.28.254.254 (IP range) Workstation: 1.0.0.15 Details: Action name: Critical CPU temperature Received from: 172.28.9.220 Priority: 187 Source: ASA Facility: 39 (Local use 9)
Action name: Critical CPU temperature						
system	Environment	Modified	172.28.9.220	172.28.9.220	8/17/2018 11:29:31 AM	
Action name: Power supply failure						
system	Environment	Modified	172.28.9.220	172.28.9.220	8/2/2018 10:01:08 AM	
Action name: Cooling fan failure						

#5: Scanning Threats

Subnet scanning and host scanning are not inherently hostile processes for learning about a network's structure and behavior, but attackers often use them to conduct reconnaissance before trying to breach a network and steal sensitive data. Netwrix Auditor tracks these actions and helps you investigate potential incidents by answering questions such as:

- ✓ Which host and subnet were scanned?
- ✓ When was each scanning attempt performed?
- ✓ Which IP address was the scanning initiated from?
- ✓ How many scanning attempts were made from each IP address?

← Search
WHO
ACTION
WHAT
WHEN
WHERE
Tools

Data source "Network Devices" ×
 Object type "Subnet" × "Host" ×
 Action "Read" ×

Open in new window
SEARCH
Advanced mode

Who	Object type	Action	What	Where	When	Details
system	Subnet	Read	100.0.0.0	172.28.9.220	9/03/2018 11:24:58 AM	Activity record details Data source: Network Devices Monitoring plan: CISCO ASA Visibility Plan Item: 172.28.0.0 – 172.28.254.254 (IP range) Details: Action name: Subnet scanning detected Received from: 172.28.9.220 Total: 2028 Burst: 200 Priority: 166 Average: 3
system	Subnet	Read	100.0.0.0	172.28.9.220	9/03/2018 11:24:51 AM	
system	Host	Read	175.0.0.1	172.28.9.220	9/03/2018 11:24:47 AM	

About Netwrix Corporation

Netwrix Corporation is a software company focused exclusively on providing IT security and operations teams with pervasive visibility into user behavior, system configurations and data sensitivity across hybrid IT infrastructures to protect data regardless of its location. Over 9,000 organizations worldwide rely on Netwrix to detect and proactively mitigate data security threats, pass compliance audits with less effort and expense, and increase the productivity of their IT teams. Founded in 2006, Netwrix has earned more than 140 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

Netwrix Auditor is a visibility platform for user behavior analysis and risk mitigation that enables control over changes, configurations and access in hybrid IT environments to protect data regardless of its location. The platform provides security intelligence to identify security holes, detect anomalies in user behavior and investigate threat patterns in time to prevent real damage.

Netwrix Auditor includes applications for Active Directory, Azure AD, Exchange, Office 365, Windows file servers, EMC storage devices, NetApp filer appliances, SharePoint, Oracle Database, SQL Server, VMware, Windows Server and Network Devices. Empowered with a RESTful API and user activity video recording, the platform delivers visibility and control across all of your on-premises and cloud-based IT systems in a unified way.

For more information, visit www.netwrix.com.



On-Premises Deployment

Download a free 20-day trial

netwrix.com/go/freetrial



Virtual Appliance

Download our virtual machine image

netwrix.com/go/appliance



Cloud Deployment

Deploy Netwrix Auditor in the cloud

netwrix.com/go/cloud

Corporate Headquarters:

300 Spectrum Center Drive, Suite 200, Irvine, CA 92618

Phone: 1-949-407-5125

Toll-free: 888-638-9749

EMEA: +44 (0) 203-588-3023



netwrix.com/social