

Топ-5 инцидентов
с сетевыми устройствами,
которые нужно
контролировать

Содержание

1. Изменения конфигурации	3
2. Неоднократные неудачные попытки входа в систему	4
3. Вход в систему с помощью VPN	5
4. Сбои в работе оборудования	6
5. Угрозы сканирования	7
О Netwrix Corporation	8

1. Изменения конфигурации

Вам необходимо отслеживать все изменения конфигурации сетевых устройств: протоколы, порты, ограничения для подключения и т. д. Любое несанкционированное или ненадлежащее изменение может вызвать проблемы с подключением, в том числе привести к полной недоступности сети. Вам также необходимо сразу же получать уведомления о том, что кто-то изменил групповую политику или создал нового пользователя, поскольку это может быть признаком инсайдерской атаки или злоупотребления полномочиями. Netwrix Auditor отслеживает как успешные, так и неудачные попытки изменения конфигурации, позволяя быстро найти ответ на следующие вопросы:

1. Кто сбросил настройки конфигурации определенного сетевого устройства?
2. Какие настройки брандмауэра были изменены?
3. С какого IP-адреса поступила команда на перезагрузку?
4. Когда был сброшен пароль маршрутизатора?

The screenshot shows the Netwrix Auditor search interface. At the top, there are navigation tabs: WHO, ACTION, WHAT, WHEN, and WHERE. Below these are search filters for Data source, Object type, Action, and Where. The search results are displayed in a table with columns: Who, Object type, Action, What, Where, and When. A details panel on the right shows activity record details for the selected row.

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. Неоднократные неудачные попытки входа в систему

Крайне важно отслеживать успешные попытки входа в систему на сетевых устройствах, чтобы проверить, действительно ли пользователь имеет соответствующие права. Однако не менее важно отслеживать неоднократные неудачные попытки входа: они могут означать, что кто-то пытается методом перебора узнать пароль администратора. Если злоумышленники получают доступ к сетевому устройству, они смогут контролировать весь сетевой трафик и похитить конфиденциальные данные. Netwrix Auditor отслеживает как успешные, так и неудачные попытки входа в систему, позволяя выявить возможные атаки методом перебора и быстро найти ответ на следующие вопросы:

1. Кто превысил максимально допустимое число последовательных неудачных попыток входа в систему?
2. Что стало причиной ошибок при входе в систему?
3. С какого IP-адреса были сделаны эти попытки?
4. Сколько попыток было предпринято?
5. Когда были сделаны неудачные запросы аутентификации?
6. На каком устройстве пользователь пытался войти в систему?

The screenshot shows a search interface with filters for Data source: "Network Devices", Object type: "Logon", and Action: "Failed logon". The results table lists three failed logon attempts for Mitch Anderson from workstation 1.2.0.10. The details panel on the right shows activity record details including monitoring plan, item, workstation, and action details.

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) 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. Вход в систему с помощью VPN

Администраторы редко входят в систему на сетевых устройствах удаленно, поэтому важно отслеживать попытки входа с помощью VPN. Более того, даже авторизованное устройство с безопасным подключением к корпоративной сети можно взломать и использовать для получения доступа к конфиденциальным файлам. Netwrix Auditor позволяет отслеживать как успешные, так и неудачные попытки входа в систему на сетевых устройствах через VPN и находить ответы на следующие вопросы:

1. Кто пытался получить доступ к сетевым устройствам с помощью VPN?
2. С какого IP-адреса были сделаны попытки аутентификации?
3. Что стало причиной ошибок при входе в систему с помощью VPN?
4. Когда были сделаны неудачные попытки входа в систему с помощью VPN?
5. На каком устройстве пользователь пытался войти в систему?

The screenshot shows the Netwrix Auditor search interface. At the top, there are navigation tabs: WHO, ACTION, WHAT, WHEN, WHERE, and Tools. Below these, search filters are set to 'Data source: Network Devices' and 'Object type: Authentication'. A 'SEARCH' button and 'Advanced mode' toggle are visible. The main table displays three authentication events for user 'Nancy Andrews'.

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	

4. Сбои в работе оборудования

Помимо отслеживания изменений в конфигурации сетевых устройств, необходимо также следить за состоянием оборудования. Если условия окружающей среды или питание сетевого устройства не соответствуют техническим требованиям, это может привести к перегреву устройства, отказу вентиляции или потере мощности с последующим снижением производительности или даже полной остановкой работы сети. Netwrix Auditor отслеживает состояние оборудования и оповещает о критических сбоях в его работе, позволяя найти ответ на следующие вопросы:

1. Какие действия были выполнены перед отключением сетевого устройства?
2. Какая часть сетевого устройства была повреждена?
3. Когда температура достигла критического уровня?

The screenshot shows the Netwrix Auditor search interface. At the top, there are navigation tabs: WHO, ACTION, WHAT, WHEN, WHERE, and Tools. Below these is a search filter bar with the following filters: Data source: "Network Devices", Object type: "RAM", "CPU", "Environment", Action: "Modified". A "SEARCH" button and "Advanced mode" toggle are also visible.

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. Угрозы сканирования

Сканирование подсетей и хостов не обязательно имеет целью изучение структуры сети и поведения устройств с целью нанесения вреда, однако оно часто используется в разведывательных целях перед попыткой взлома сети и похищения конфиденциальных данных. Netwrix Auditor отслеживает эти действия и позволяет расследовать возможные инциденты и найти ответы на следующие вопросы:

1. Сканирование какого хоста или подсети было выполнено?
2. Когда были сделаны попытки сканирования?
3. С какого IP-адреса было запущено сканирование?
4. Сколько попыток сканирования было сделано с каждого IP-адреса?

The screenshot shows the Netwrix Auditor search interface. The search criteria are: Data source: "Network Devices", Object type: "Subnet" and "Host", Action: "Read". The results table shows three entries for "Subnet scanning detected" and one for "Host scanning detected".

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	

О Netwrix Corporation

Компания Netwrix Corporation разрабатывает ПО, которое обеспечивает ИТ-отделам и отделам информационной безопасности возможности полного контроля поведения пользователей, конфигураций систем и конфиденциальности данных в любых гибридных ИТ-инфраструктурах, позволяя защитить данные, где бы они ни находились. Более 9000 организаций в разных странах используют решения Netwrix для выявления и своевременного устранения угроз безопасности данных, прохождения аудита на соответствие стандартам с меньшими затратами сил и средств, а также повышения эффективности работы ИТ-отделов. Компания Netwrix была основана в 2006 году. Она удостоена более чем 140 отраслевых наград и включена в списки самых быстрорастущих компаний в США «Inc. 5000» и «Deloitte Technology Fast 500».

Netwrix Auditor — это платформа, которая обеспечивает анализ поведения пользователей и снижение рисков, позволяя контролировать изменения, конфигурации и права доступа в гибридных ИТ-инфраструктурах для защиты данных, где бы они ни находились. Платформа обеспечивает сбор информации о безопасности для выявления уязвимостей и подозрительного поведения пользователей, а также своевременного расследования потенциальных угроз с целью предотвращения реального ущерба.

Netwrix Auditor включает в себя приложения для Active Directory, Azure AD, Exchange, Office 365, файловых серверов Windows, систем хранения данных EMC и NetApp, SharePoint, Oracle Database, SQL Server, VMware, Windows Server и сетевых устройств. Благодаря интеграции с RESTful API и возможности видеозаписи действий пользователей платформа обеспечивает полный контроль ситуации на локальной площадке и в облачных инфраструктурах.

Подробную информацию можно найти на веб-сайте www.netwrix.ru.



Локальное развертывание

Загрузите 20-дневную пробную версию бесплатно

netwrix.ru/auditor.html



Виртуальное устройство

Загрузите образ виртуальной машины

netwrix.com/go/appliance



Облачное развертывание

Разверните Netwrix Auditor в облаке

netwrix.com/go/cloud