

Security Events

<https://campus.barracuda.com/doc/46208966/>

The following article provides an overview on all security events that are processed by the Barracuda NextGen Firewall F-Series.

Event-ID	Description	Relevance	Severity	Notification	Persistent
53	Duplicate IP Detected	An IP address living on the system has additionally been detected in the network.	Warning	2	yes
140	Mail Size Limit Exceeded	The size of an e-mail has exceeded the configured limit (see:). This event is only reported when parameter Limit Mail Data Size is set to yes .	Notice	2	no
300	User ID (UID) Invalid	Invalid system user ID. See log for details.	Security	3	no
304	Reserved Login ID Used	Apple notification. Apple ID was used to sign in to a device.	Security	3	no
2400	Config Node Change Notice	A configuration file has been edited in the Barracuda NextGen Control Center configuration tree. "Config node change" events are only reported if event notification has been configured for configuration file changes (CC context menu entry Properties ...). The following events apply: <ul style="list-style-type: none"> • Normal Event - Event-ID 2400 • Notice Event - Event-ID 2401 • Alert Event - Event-ID 2402 	Notice	2	no
2401	Config Node Change Warning		Warning	2	no
2402	Config Node Change Alert		Security	3	no

2420	NextGen Firewall F-Series Login Notice	An application has been granted administrative access to the system. Barracuda Networks applications generate "Barracuda Networks Subsystem Login" notifications every time a user has successfully logged into an application that interacts with the graphical administration tool Barracuda NextGen Admin (for example control, event, statistics, config). The severity level for notifications regarding access to box services is configurable in CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification ; Notifications for other services may be customized per service.	Notice	2	no
2421	NextGen Firewall F-Series Login Warning		Warning	2	no
2422	NextGen Firewall F-Series Login Alert		Security	3	no
2510	FW Global Connection Limit Exceeded	The number of total sessions allowed for a request has been exceeded (see: General Firewall Configuration).	Security	3	yes
2600	DHCP Lease Deleted	A DHCP lease has been deleted from the database.	Notice	2	no
3011	CRL Collection Failed	Collection of the Certificate Revocation List (CRL) has failed. Paths to CRLs are defined in the VPN Settings > Root Certificates tab > Certificate Revocation tab (see:). Polling for CRL retrieval is defined through parameter CRL Poll Time .	Security	3	no
3012	VPN Client Version	Connection refused due to invalid VPN Client version.	Warning	2	no
3013	Antivir Pattern Update Failed	Update to the recent Virus Scanner definitions has not succeeded.	Security	3	no
4000	FW Port Scan Detected	The number of blocked requests has exceeded the Port Scan Threshold within the configured Port Scan Detection Interval. Limit values can be customized in the Firewall Settings > Reporting tab.	Notice	2	no

4002	FW Flood Ping Protection Activated	The Min Delay time for pinging defined in a Firewall Service Object (see:) has been under-run and the connection has therefore been blocked by the FW.	Warning	2	no
4004	FW Activating Perimeter Defence (inbound mode)	The Inbound Mode Threshold (%) value specified in the Local Firewall settings (see: Host Firewall) has been exceeded.	Security	3	no
4006	FW Pending TCP Connection Limit Reached	The number of pending TCP sessions per source IP exceeds the allowed maximum. Requests initiating further pending sessions will be blocked. The threshold is configurable in the Firewall Forwarding Settings > Firewall tab (parameter Max. Pending Forward Accepts/Src).	Security	3	no
4008	FW UDP Connection per Source Limit Exceeded	The maximum number of UDP sessions per source IP has been exceeded. The thresholds can be configured in the Local Firewall Settings > Session Limits tab (parameter Max Local-In UDP/Src) and in the Firewall Forwarding Settings > Firewall tab (parameter Max. Forwarding UDP/Src).	Warning	2	no
4009	FW UDP Connection Limit Exceeded	The maximum number of UDP sessions has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter Max UDP (%)).	Security	3	no
4010	FW Oversized SYN Packet Dumped	An oversized SYN packet has been dropped by the firewall.	Notice	2	no
4012	FW Large ICMP Packet Dumped	An ICMP-ECHO packet larger than the configured Max Ping Size (see: Service Objects) has been dropped by the firewall.	Notice	2	no
4014	FW IP Spoofing Attempt Detected	An IP spoofing attempt has been discovered.	Notice	4	no

4015	FW Potential IP Spoofing Attempt	A SYN flooding attack has been identified (see: Best Practice - Protect Against TCP SYN Flooding Attacks with TCP Accept Policies).	Notice	4	no
4016	FW Rule Connection Limit Exceeded	The maximum number of concurrent connections allowed per rule has been exceeded. The maximum value is defined by parameter Max. Number of Sessions (see: General Firewall Configuration).	Warning	2	no
4018	FW Rule Connection per Source Limit Exceeded	The maximum number of concurrent connections allowed per rule and source has been exceeded. The maximum value is defined by parameter Max. Number of Sessions per Source (see: General Firewall Configuration).	Warning	2	no
4020	FW Rule Notice	A firewall rule equipped with event generation has been processed. The severity level of the generated event is defined by the rule (see: How to Configure Event Notifications).	Notice	2	no
4021	FW Rule Warning	A firewall rule generating event log type `warning` has been processed.	Warning	2	no
4022	FW Rule Alert	A firewall rule generating event log type `alert` has been processed.	Security	3	no
4024	FW Global Connection per Source Limit Exceeded	The maximum number of concurrent connections allowed per source has been exceeded. The maximum value is defined by parameters Max Local-In Session/Src in the Local Firewall Settings and Max. Forwarding Session/Src in the Forwarding Firewall Settings .	Warning	2	no

4026	FW ICMP-ECHO Connection per Source Limit Exceeded	The maximum number of concurrent ICMP-ECHO connections allowed per source has been exceeded. The maximum value is defined by parameters Max Local-In Echo/Src in the Local Firewall Settings and Max. Forwarding Echo/Src in the Forwarding Firewall Settings .	Warning	2	no
4027	FW ICMP-ECHO Connection Limit Exceeded	The maximum number of ICMP-ECHO connections has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter Max Echo (%)) (see: General Firewall Configuration).	Warning	2	no
4028	FW OTHER-IP Connection per Source Limit Exceeded	The maximum number of concurrent OTHER-IP connections (all IP protocols except TCP, UDP and ICMP) allowed per source has been exceeded. The maximum value is defined by parameters Max Local-In Other/Src in the Local Firewall Settings and Max. Forwarding Other/Src in the Forwarding Firewall Settings .	Warning	2	no
4029	FW OTHER-IP Session Limit Exceeded	The maximum number of OTHER-IP sessions (all IP protocols except TCP, UDP and ICMP) has been exceeded. The threshold can be configured in the Local Firewall Settings > Session Limits tab (parameter Max Other (%)).	Warning	2	no
4050	FW ARP MAC Address Changed	ARP has detected a MAC address change.	Notice	2	no
4051	FW ARP Ambiguous Duplicate Reply	ARP has detected a duplicate MAC address.	Notice	2	no
4052	FW ARP Request Device Mismatch	ARP has detected a device mismatch.	Notice	2	no

4053	FW ARP Reverse Routing Interface Mismatch	ARP has detected an interface mismatch.	Notice	2	no
4060	IPS Log Notice	IPS Signature. An object of event log type `Notice' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Notice	666	no
4061	IPS Log Warning	IPS Signature. An object of event log type `Warning' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Warning	666	no
4062	IPS Log Alert	IPS Signature. An object of event log type `Alert' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Security	666	no
4063	IPS Drop Notice	IPS Signature. An object of event log type `Drop Notice' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Notice	666	no
4064	IPS Drop Warning	IPS Signature. An object of event log type `Drop Warning' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Warning	666	no
4065	IPS Drop Alert	IPS Signature. An object of event log type `Drop Alert' referenced in the Intrusion Prevention System (IPS) database has been detected by the firewall.	Security	666	no
4100	User Unknown	A system login has been attempted with an unknown login ID (CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification , see: How to Configure Access Notifications).	Warning	2	no
4110	Authentication Failure Notice	A login attempt with a valid login ID has failed (CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification , see: How to Configure Access Notifications).	Notice	2	no

4111	Authentication Failure Warning	A login attempt with a valid login ID has failed the second time (CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification , see: How to Configure Access Notifications). The ACL does not match (see: , - Allowed Phone Numbers).	Warning	2	no
4112	Authentication Failure Alert	A login attempt with a valid login ID has failed at least three times (CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification , see: How to Configure Access Notifications). Password authentication failure and/or unsuccessful command match (see: , - Command Codes).	Security	3	no
4120	Session Opened Notice	Informal event stating that a firewall session has been initiated.	Notice	2	no
4121	Session Opened Warning	A traced user has initiated an SSH connection (see: - Recorded Users).	Warning	2	no
4122	Session Opened Alert	A firewall session has been initiated. See log for details.	Security	3	no
4124	Remote Command Execution Notice	Remote command execution has been triggered remotely by the Barracuda NextGen Control Center (in CC CONTROL > Remote Execution) or by an authorized user. Note that copying files with SCP also generates this event. Successful authentication and command is accepted (see: , - Command Codes).	Notice	2	no
4125	Remote Command Execution Warning	Remote command execution of event log type 'warning' has been triggered.	Warning	2	no
4126	Remote Command Execution Alert	Remote command execution of event log type `alert` has been triggered.	Security	3	no

4130	System Login Notice	<p>The quality of these event notifications is determined by the settings made in CONFIGURATION > Configuration Tree > Box > Advanced Configuration > Access Notification (see: How to Configure Access Notifications).</p> <p>The following notifications apply with default settings:</p> <ul style="list-style-type: none"> • Notice (not assigned) • Warning (successful SSH and remote SSH login) • Alert (successful console login). <p>Login failure triggers events 4110, 4111, and 4112 (see above).</p>	Notice	2	no
4131	System Login Warning		Warning	2	no
4132	System Login Alert		Security	3	no
4160	Log Data Deleted	One or more entries have been deleted from the log database. See log for details.	Notice	2	no
4162	Statistics Data Deleted	One or more entries have been deleted from the statistics database. See log for details.	Notice	2	no
4163	Statistics Collection Failed	CC Statistics Collection has failed for a range, cluster, or box service. See statistics services, CC Control > Statistics Collection , and log for details.	Notice	2	no
4200	CTRL-ALT-DEL	Keyboard combination CTRL-ALT-DEL has been used on Barracuda Firewall Admin to shut down or reboot a firewall.	Warning	2	no
4202	System Reboot	The system has been rebooted. Manual reboot will trigger this event just like the Watchdog repair binary (see: Watchdog).	Warning	2	no
4204	System Shutdown	The system has been shut down.	Warning	2	no
4206	Runlevel Changed	The runlevel of the operating system has changed. Runlevels change during system boot.	Notice	2	no
4210	Single User Mode	The system has been booted in Single User mode using the boot option "single".	Warning	2	no

4212	Problems During Bootup	Unusual behavior of the firewall during bootup process. See log for details.	Warning	2	no
4214	Incomplete Previous Boot	The previous system bootup could not be completed.	Warning	2	no
4220	System Boot	The system is starting the bootup process.	Notice	2	no
4222	Emergency System Boot	An emergency system boot has been executed. See log for details.	Warning	2	no
4240	Bootloader Configuration Change	A configuration change has been applied to the bootloader configuration. See log for details.	Notice	2	no
4242	Two Phase Kernel Update	New kernels installed during update. See log for details.	Notice	2	no
4244	Automatic Kernel Update	New kernels installed during update. See log for details.	Notice	2	no
4246	Kernel Update Rejected	Kernel update has failed. See log for details.	Warning	2	no
4248	Custom Bootloader or Kernel Update	Bootloader or kernel was updated. See log for details.	Notice	2	no
4250	Bootloader Test Activation Failure	Bootloader test activation has errors or failed. See log for details.	Notice	2	no
4252	Bootloader Activation Failed	Bootloader activation has failed. See log for details.	Warning	2	no
4254	Bootloader Disaster Recovery	Bootloader disaster recovery was performed. See log for details.	Warning	2	no
4256	Bootloader Reconfigured	A new configuration has been applied to the bootloader. See log for details.	Notice	2	no
4258	Kernel Update	Kernel update was performed. See log for details.	Warning	2	no
4260	Pending Kernel Update	Kernel update is waiting for installation. See log for details.	Warning	2	no
4261	Activate Pending Kernel Update	Kernel update is waiting for activation. See log for details.	Warning	2	no
4262	Bootloader Reconfiguration Failed	Bootloader configuration update has failed. See log for details.	Warning	2	no

4264	Kernel Update Failed	Kernel update has failed. See log for details.	Warning	2	no
4300	Empty ACL Encountered	Access Control List (ACL) contains empty values. See log for details.	Security	3	no
4302	Overlong ACL Encountered	Access Control List (ACL) contains too many values. See log for details.	Security	3	no
4304	Password Update Failure	Password or key update failed. See log for details.	Security	3	no
4306	Password Updated	The password of the support user or the user "root" has changed.	Warning	2	no
4307	Key Updated	The root public RSA key has changed.	Warning	2	no
4400	Release Update Triggered	Software update has been triggered manually.	Notice	2	no
4402	Subsystem Release Update Succeeded	NextGen Firewall successfully updated. See log for details.	Notice	2	no
4404	Subsystem Release Update Cancelled	A software update has been cancelled.	Notice	2	no
4406	Subsystem Release Update Aborted	A software update has been aborted. See log for details.	Warning	2	no
4408	Release Update Failed	A NextGen Firewall release update has failed. See log for details.	Security	3	no
4410	Release Inconsistencies Detected	Incorrect RPM packages have been installed, for example hotfixes intended for another Barracuda NextGen Firewall F-Series release version, or Barracuda Networks files have been modified, for example by manually editing a Barracuda Networks script.	Warning	2	no
4412	Active Kernel not in RPM-DB	The Linux Kernel in use has not been added to the RPM database.	Notice	2	no
4450	New Barracuda Software Update	A new software update from Barracuda Networks is available. See DASHBOARD General Page	Notice	2	yes
4460	New Product Tip	A new Product Tip from Barracuda Networks is available. See DASHBOARD General Page	Notice	2	yes

4500	Mail Data Discarded	An e-mail has been discarded from the mail queue (see: - Mail Queue Tab, Discard Mail . This event is only reported when parameter Admin Reception Commands (see:) is set to yes .	Notice	2	no
4504	Mail Operation Changed	An e-mail has been allowed or blocked manually (Processes Tab, Allow Mail Reception/Block Mail Reception). This event is only reported when parameter Admin Discard Mail Cmd is set to yes .	Notice	2	no
4506	Mail Delivery Refused	E-mail delivery to a banned recipient has been refused. This event is only reported when parameter Recipient Dropped is set to yes .	Notice	2	no
4508	Mail Relaying Denied	Relaying of an e-mail has been denied according to content filter configuration. This event is only reported when parameter Mail Denied (see:) is set to yes .	Notice	2	no
4512	Mail Rule Notice	These are customized events with corresponding customized descriptions, which are triggered when Action type 'Event' is used. <ul style="list-style-type: none"> • Event-ID 0 = Severity Notice • Event-ID 1 = Severity Warning • Event-ID 2 = Severity Security Events will only be reported when parameter User Defined Rule Event is set to yes (default).	Notice	2	no
4513	Mail Rule Warning		Warning	2	no
4514	Mail Rule Alert		Security	3	no
4600	Attempted Illegal Assignment	While processing data provided by dhcpd, a potentially malign assignment <code>\${KEY} = ->\${VAL}<--</code> has been detected.	Security	3	no
5000	User added to ATD quarantine	A user or IP address has been added to the ATP quarantine network object.	Warning	1	yes
5001	ATD malicious activity detected	A file considered to be malicious has been detected by ATP.	Warning	1	yes
5002	ATD Cloud status	Firewall connection to the ATP Cloud - primary ATP server cannot be reached, switching over to secondary server.	Security	2	yes

5003	ATD Cloud status	Firewall connection to the ATP Cloud - connection to primary and secondary ATP server failed due to latency or overload.	Warning	2	yes
5004	DNS Sinkhole address accessed	A client has accessed the DNS sinkhole address. This may point to a potential infection of the client.	Warning	1	yes

© Barracuda Networks Inc., 2020 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.