BIG-IP® Systems: DoS Protection and Protocol Firewall Implementations

Version 11.6

Table of Contents

Legal Notices

Publication Date

This document was published on August 20, 2014.

Publication Number

MAN-0440-03

Copyright

Trademarks

Patents

This product may be protected by one or more patents indicated at:
http://www.f5.com/about/guidelines-policies/patents

Export Regulation Notice

This product may include cryptographic software. Under the Export Administration Act, the United States government may consider it a criminal offense to export this product from the United States.

RF Interference Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This unit generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Any modifications to this device, unless expressly approved by the manufacturer, can void the user's authority to operate this equipment under part 15 of the FCC rules.

Canadian Regulatory Compliance

This Class A digital apparatus complies with Canadian ICES-003.

Standards Compliance

This product conforms to the IEC, European Union, ANSI/UL and Canadian CSA standards applicable to Information Technology products at the time of manufacture.

Acknowledgments

This product includes software developed by Bill Paul.

This product includes software developed by Jonathan Stone.

This product includes software developed by Manuel Bouyer.

This product includes software developed by Paul Richards.

This product includes software developed by the NetBSD Foundation, Inc. and its contributors.

This product includes software developed by the Politecnico di Torino, and its contributors.

This product includes software developed by the Swedish Institute of Computer Science and its contributors.

This product includes software developed by the University of California, Berkeley and its contributors.

This product includes software developed by the Computer Systems Engineering Group at the Lawrence Berkeley Laboratory.

This product includes software developed by Christopher G. Demetriou for the NetBSD Project.

This product includes software developed by Adam Glass.

This product includes software developed by Christian E. Hopps.

This product includes software developed by Dean Huxley.

This product includes software developed by John Kohl.

This product includes software developed by Paul Kranenburg.

This product includes software developed by Terrence R. Lambert.

This product includes software developed by Philip A. Nelson.

This product includes software developed by Herb Peyerl.

This product includes software developed by Jochen Pohl for the NetBSD Project.

This product includes software developed by Chris Provenzano.

This product includes software developed by Theo de Raadt.

This product includes software developed by David Muir Sharnoff.

This product includes software developed by SigmaSoft, Th. Lockert.

This product includes software developed for the NetBSD Project by Jason R. Thorpe.

This product includes software developed by Jason R. Thorpe for And Communications, http://www.and.com.

This product includes software developed for the NetBSD Project by Frank Van der Linden.

This product includes software developed for the NetBSD Project by John M. Vinopal.

This product includes software developed by Christos Zoulas.

This product includes software developed by the University of Vermont and State Agricultural College and Garrett A. Wollman.

This product includes software developed by Balazs Scheidler (bazsi@balabit.hu), which is protected under the GNU Public License.

This product includes software developed by Niels Mueller (nisse@lysator.liu.se), which is protected under the GNU Public License.

In the following statement, "This software" refers to the Mitsumi CD-ROM driver: This software was developed by Holger Veit and Brian Moore for use with 386BSD and similar operating systems. "Similar operating systems" includes mainly non-profit oriented systems for research and education, including but not restricted to NetBSD, FreeBSD, Mach (by CMU).

This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).

This product includes software licensed from Richard H. Porter under the GNU Library General Public License (© 1998, Red Hat Software), www.gnu.org/copyleft/lgpl.html.

This product includes the standard version of Perl software licensed under the Perl Artistic License (© 1997, 1998 Tom Christiansen and Nathan Torkington). All rights reserved. You may find the most current standard version of Perl at http://www.perl.com.

This product includes software developed by Jared Minch.

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product contains software based on oprofile, which is protected under the GNU Public License.

This product includes RRDtool software developed by Tobi Oetiker (http://www.rrdtool.com/index.html) and licensed under the GNU General Public License.

This product contains software licensed from Dr. Brian Gladman under the GNU General Public License (GPL).

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

This product includes Hypersonic SQL.

This product contains software developed by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and others.

This product includes software developed by the Internet Software Consortium.

This product includes software developed by Nominum, Inc. (http://www.nominum.com).

This product contains software developed by Broadcom Corporation, which is protected under the GNU Public License.

This product contains software developed by MaxMind LLC, and is protected under the GNU Lesser General Public License, as published by the Free Software Foundation.

This product includes Intel QuickAssist kernel module, library, and headers software licensed under the GNU General Public License (GPL).

This product includes software licensed from Gerald Combs (gerald@wireshark.org) under the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or any later version. Copyright ©1998 Gerald Combs.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM,

Chapter 1

Detecting and Protecting Against DoS, DDoS, and Protocol Attacks

About detecting and protecting against DoS, DDoS, and protocol attacks

Attackers can target the BIG-IP® system in a number of ways. The BIG-IP system addresses several possible DoS, DDoS, SIP, and DNS attack routes. These DoS attack prevention methods are available when the Advanced Firewall Manager™ is licensed and provisioned.

DoS and DDoS attacks

Denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks attempt to render a machine or network resource unavailable to users. DoS attacks require the efforts of one or more people to disrupt the services of a host connected to the Internet. The Advanced Firewall Manager allows you to configure packet limits, percentage increase thresholds, and absolute rate limits of a wide variety of packets that attackers leverage as attack vectors, to detect and prevent attacks of this type. Configure responses to such attacks in the Device DoS profile.

DNS and SIP flood (or DoS) attacks

Denial-of-service (DoS) or flood attacks attempt to overwhelm a system by sending thousands of requests that are either malformed or simply attempt to overwhelm a system using a particular DNS query type or protocol extension, or a particular SIP request type. The BIG-IP system allows you to track such attacks, using the DoS Protection profile.

DoS Sweep and Flood attacks

A sweep attack is a network scanning technique that sweeps your network by sending packets, and using the packet responses to determine responsive hosts. Sweep and Flood attack prevention allows you to configure system thresholds for packets that conform to typical sweep or flood attack patterns. This configuration is set in the Device DoS profile.

Malformed DNS packets

Malformed DNS packets can be used to consume processing power on the BIG-IP system, ultimately causing slowdowns like a DNS flood. The BIG-IP system drops malformed DNS packets, and allows you to configure how you track such attacks. This configuration is set in the DoS Protection profile.

Malformed SIP packets

Malformed SIP request packets can be used to consume processing power on the BIG-IP system, ultimately causing slowdowns like a SIP flood. The BIG-IP system drops malformed SIP packets, and allows you to configure how you track such attacks. This configuration is set in the DoS Protection profile.

Protocol exploits

Attackers can send DNS requests using unusual DNS query types or opcodes. The BIG-IP system can be configured to allow or deny certain DNS query types, and to deny specific DNS opcodes. When you configure the system to deny such protocol exploits, the system tracks these events as attacks. This configuration is set in the DNS Security profile.

About profiles for DoS and DNS service attacks

On your BIG-IP® system, you can use different profiles to detect and protect against system DoS attacks, and specific protocol attacks for DNS and SIP.

DoS Protection profile

The DoS Protection profile allows you to configure the response thresholds on the BIG-IP system for malformed DNS and SIP packets. Malformed packets are dropped by the system. The DoS Protection profile also allows you to configure the threshold increase of packets of specific DNS query types, and

SIP request types. You can use SNMP alerts generated by these items, and information reported in real-time reports and in system logs, to mitigate a specific DNS query type attack; for example, by blocking it with the DNS security profile. You can also track SIP requests through alerts, though this is informational only.

DNS Security profile

The DNS Security profile allows you to configure the BIG-IP system to exclude (drop) or include (allow) packets of specific DNS query types. You can also configure the profile to drop specific DNS header opcodes.

Chapter 2

Detecting and Preventing System DoS and DDoS Attacks

About configuring the BIG-IP system to detect and prevent DoS and DDoS attacks

DoS and DDoS attack detection and prevention is enabled by the BIG-IP® Advanced Firewall Manager™ (AFM™) Device DoS profile. DoS and DDoS detection and prevention serves two functions. DoS detection and prevention features are enabled with an Advanced Firewall Manager license, which also includes DNS protocol detection support.

- To detect, and automatically mitigate, packets that present as DoS or DDoS attacks.
- To determine unusual increases in packets of specific types that are known attack vectors. Possible attack vectors are tracked over the past hour, and current possible attacks are compared to the average of that hour.

You can configure the levels at which a BIG-IP device detects all system-supported DoS attacks.

Detecting and protecting against DoS and DDoS attacks

The BIG-IP® system handles DoS and DDoS attacks with preconfigured responses. With the DoS Protection Device Configuration, you set detection thresholds and internal rate limits for a range of DoS and DDoS attack vectors.

1. On the Main tab, click **Security** > **DoS Protection** > **Device Configuration**.
   The DoS Protection Device Configuration screen opens.
2. If you are using remote logging, from the **Log Publisher** list, select a destination to which the BIG-IP system sends DoS and DDoS log entries.
3. In the **Category** column, expand a category to view and edit the attack types for that category.
4. In the **Attack Type** column, click the name of any attack type to edit the settings.
   The configuration page for the particular attack appears.
5. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value for the attack detection threshold. The value is determined by an average of the packets per second over the last minute. If packets of this type cross the threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is never logged or reported.
6. From the **Detection Threshold Percent** list, select **Specify** or **Infinite**.
   - Use **Specify** to set the percentage increase value, that specifies an attack is occurring. The system compares the current rate to an average rate from the last hour. For example, if the average rate for the last hour is `1000 packets per second`, and you set the percentage increase threshold to `100`, an attack is detected at 100 percent above the average, or `2000 packets per second`. When the threshold is passed, an attack is logged and reported.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is never logged or reported.
7. From the **Default Internal Rate Limit** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value, in packets per second, which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again.

- Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not rate-limited.

Important: *If a packet is determined to be an error packet, that packet is dropped, regardless of these settings.*

8. Click the **Update** button.
   The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.
9. Repeat the previous steps for any other attack types for which you want to change the configuration.

Now you have configured the system to provide custom responses to possible DoS and DDoS attacks, and to allow such attacks to be identified in system logs and reports.

Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system.

Device DoS attack types

You can specify specific threshold, rate increase, rate limit, and other parameters for supported device DoS attack types, to more accurately detect, track, and rate limit attacks.

Attention: *All hardware-supported vectors are performed in hardware on vCMP guests, as long as the vCMP guests have the same software version as the vCMP host.*

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
Bad Header - DNS	DNS Oversize	dns-oversize	Detects oversized DNS headers. To tune this value, in tmsh: `modify sys db dos.maxdnssize value`, where `value` is `256-8192`.	Yes
Bad Header - ICMP	Bad ICMP Checksum	badicmpchksum	An ICMP frame checksum is bad. Reuse the TCP or UDP checksum bits in the packet	Yes
	Bad ICMP Frame	badicmpframe	The ICMP frame is either the wrong size, or not of one of the valid IPv4 or IPv6 types. Valid IPv4 types: • 0 Echo Reply • 3 Destination Unreachable • 4 Source Quench • 5 Redirect • 8 Echo • 11 Time Exceeded • 12 Parameter Problem • 13 Timestamp • 14 Timestamp Reply • 15 Information Request • 16 Information Reply • 17 Address Mask Request • 18 Address Mask Reply Valid IPv6 types: • 1 Destination Unreachable	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
			• 2 Packet Too Big • 3 Time Exceeded • 4 Parameter Problem • 128 Echo Request • 129 Echo Reply • 130 Membership Query • 131 Membership Report • 132 Membership Reduction	
	ICMP Frame Too Large	icmp-frame-too-large	The ICMP frame exceeds the declared IP data length or the maximum datagram length. To tune this value, in tmsh: `modify sys db dos.maxicmpframesize value`, where `value` is `<=65515`.	Yes
Bad Header - IGMP	Bad IGMP Frame	bad-igmp-frame	IPv4 IGMP packets should have a header >= 8 bytes. Bits 7:0 should be either 0x11, 0x12, 0x16, 0x22 or 0x17, or else the header is bad. Bits 15:8 should be non-zero only if bits 7:0 are 0x11, or else the header is bad.	Yes
Bad Header - IPv4	Bad IP TTL Value	bad-ttl-val	Time-to-live equals zero for an IPv4 address.	Yes
	Bad IP Version	bad-ver	The IPv4 address version in the IP header is not 4.	Yes
	Header Length > L2 Length	hdr-len-gt-l2-len	No room in layer 2 packet for IP header (including options) for IPv4 address	Yes
	Header Length Too Short	hdr-len-too-short	IPv4 header length is less than 20 bytes	Yes
	Bad Source	ip-bad-src	The IPv4 source IP = `255.255.255.255` or `0xe0000000U`	Yes
	IP Error Checksum	ip-err-chksum	The header checksum is not correct	Yes
	IP Length > L2 Length	ip-len-gt-l2-len	Total length in IPv4 address header or payload length in IPv6 address header is greater than the layer 3 length in a layer 2 packet	Yes
	TTL <= <tunable>	ttl-leq-one	An IP packet with a destination that is not multicast and that has a TTL greater than 0 and less than or equal to a tunable value, which is 1 by default. To tune this value, in tmsh: `modify sys db dos.iplowttl value`, where `value` is `1-4`.	Yes
	IP Option Frames	ip-opt-frames	IPv4 address packet with `option.db variable tm.acceptipsourceroute` must be enabled to receive IP options	Yes
	IP Option Illegal Length	bad-ip-opt	Option present with illegal length	No
	L2 Length >> IP Length	l2-len-gg-ip-len	Layer 2 packet length is much greater than the payload length in an IPv4 address header and the	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
			layer 2 length is greater than the minimum packet size	
	No L4	no-l4	No layer 4 payload for IPv4 address	Yes
	Unknown Option Type	unk-ipopt-type	Unknown IP option type	No
Bad Header - IPv6	IPv6 extended headers wrong order	bad-exthdr-order	Extension headers in the IPv6 header are in the wrong order	Yes
	Bad IPV6 Hop Count	bad-ipv6-hopcnt	Both the terminated (cnt=0) and forwarding packet (cnt=1) counts are bad.	Yes
	Bad IPV6 Version	bad-ipv6-ver	The IPv6 address version in the IP header is not 6	Yes
	IPv6 duplicate extension headers	dup-ext-hdr	An extension header should occur only once in an IPv6 packet, except for the Destination Options extension header.	Yes
	IPv6 extension header too large	exthdr-too-large	An extension header is too large. To tune this value, in tmsh: `modify sys db dos.maxipv6extsize value`, where `value` is `0-1024`.	Yes
	IPv6 hop count <= <tunable>	hopcnt-low	The IPv6 extended header hop count is less than or equal to <tunable>. To tune this value, in tmsh: `modify sys db dos.ipv6lowhopcnt value`, where `value` is `1-4`.	Yes
	Bad IPv6 source	ipv6-bad-src	IPv6 source IP = `0xff00::`	Yes
	IPV6 Extended Header Frames	ipv6-exthdr-frames	IPv6 address contains extended header frames	Yes
	IPV6 Length > L2 Length	ipv6-length-l2-len	IPv6 address length is greater than the layer 2 length	Yes
	IPV6 Source Address == Destination Address		IPv6 packet source address is the same as the destination address	Yes
	No L4 (Extended Headers Go To Or Past End of Frame)	l4-exthdrs-end	Extended headers go to the end or past the end of the L4 frame	Yes
	Payload Length < L2 Length	payload-l2-len	Specified IPv6 payload length is less than the L2 packet length	Yes
	Too Many Extended Headers	too-many-exthdrs	For an IPv6 address, there are more than <tunable> extended headers (the default is `4`). To tune this value, in tmsh: `modify sys db dos.maxipv6exthdrs value`, where `value` is `0-15`.	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
Bad Header - L2	Ethernet MAC Source Address == Destination Address	[illegible]	Ethernet MAC source address equals the destination address.	Yes
Bad Header - TCP	Bad TCP Checksum	[illegible]	The TCP checksum does not match	Yes
	Bad TCP Flags (All Cleared)	[illegible]	Bad TCP flags (all cleared and SEQ#=0)	Yes
	Bad TCP Flags (All Flags Set)	[illegible]	Bad TCP flags (all flags set)	Yes
	FIN Only Set	fin-only-set	Bad TCP flags (only FIN is set)	Yes
	Option Present With Illegal Length	[illegible]	Option present with illegal length	Yes
	SYN && FIN Set	syn-and-fin-set	Bad TCP flags (SYN and FIN set)	Yes
	TCP Flags - Bad URG	tcp-bad-urg	Packet contains a bad URG flag, this is likely malicious	Yes
	TCP Header Length > L2 Length	[illegible]		Yes
	TCP Header Length Too Short (Length < 5)	[illegible]	The Data Offset value in the TCP header is less than five 32-bit words	Yes
	TCP Option Overruns TCP Header	[illegible]	The TCP option bits overrun the TCP header.	Yes
	Unknown TCP Option Type	[illegible]	Unknown TCP option type	Yes
Bad Header - UDP	Bad UDP Checksum	[illegible]	The UDP checksum is not correct	Yes
	Bad UDP Header (UDP Length > IP Length or L2 Length)	bad-udp-hdr	UDP length is greater than IP length or layer 2 length	Yes
DNS	DNS AAAA Query	dns-aaaa-query	UDP packet, DNS Qtype is AAAA, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS Any Query	dns-any-query	UDP packet, DNS Qtype is ANY_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
	DNS AXFR Query	dns-axfr-query	UDP packet, DNS Qtype is AXFR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS A Query	dns-a-query	UDP packet, DNS Qtype is A_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS CNAME Query	dns-cname-query	UDP DNS query, DNS Qtype is CNAME, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS IXFR Query	dns-ixfr-query	UDP DNS query, DNS Qtype is IXFR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS Malformed	dns-malformed	Malformed DNS packet	Yes
	DNS MX Query	dns-mx-query	UDP DNS query, DNS Qtype is MX, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS NS Query	dns-ns-query	UDP DNS query, DNS Qtype is NS, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS OTHER Query	dns-other-query	UDP DNS query, DNS Qtype is OTHER, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS PTR Query	dns-ptr-query	UDP DNS query, DNS Qtype is PTR, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS QDCount Limit	dns-qdcount-limit	UDP packet, DNS qdcount neq 1, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS Response Flood	dns-response-flood	UDP DNS Port=53, packet and DNS header flags bit 15 is 1 (response), VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.;	Yes
	DNS SOA Query	dns-soa-query	UDP packet, DNS Qtype is SOA_QRY, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS SRV Query	dns-srv-query	UDP packet, DNS Qtype is SRV, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
	DNS TXT Query	dns-txt-query	UDP packet, DNS Qtype is TXT, VLAN is <tunable>. To tune this value, in tmsh: `modify sys db dos.dnsvlan value`, where `value` is `0-4094`.	Yes
Flood	ARP Flood	arp-flood	ARP packet flood	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
	Ethernet Broadcast Packet	ether-bcst-pkt	Ethernet broadcast packet flood	Yes
	Ethernet Multicast Packet	ether-mcst-pkt	Ethernet destination is not broadcast, but is multicast	Yes
	ICMPv4 Flood	icmpv4-flood	Flood with ICMP v4 packets	Yes
	ICMPv6 Flood	icmpv6-flood	Flood with ICMP v6 packets	Yes
	IGMP Flood	igmp-flood	Flood with IGMP packets (IPv4 packets with IP protocol number 2)	Yes
	IGMP Fragment Flood	igmp-frag-flood	Fragmented packet flood with IGMP protocol	Yes
	IPv4 Fragment Flood	ip-frag-flood	Fragmented packet flood with IPv4	Yes
	IPv6 Fragment Flood	ipv6-frag-flood	Fragmented packet flood with IPv6	Yes
	Routing Header Type 0	routing-header-type-0	Routing header type zero is present in flood packets	Yes
	TCP BADACK Flood	tcp-ack-flood	TCP ACK packet flood	No
	TCP RST Flood	tcp-rst-flood	TCP RST flood	Yes
	TCP SYN ACK Flood	tcp-synack-flood	TCP SYN/ACK flood	Yes
	TCP SYN Flood	tcp-syn-flood	TCP SYN flood	Yes
	TCP Window Size	tcp-window-size	The TCP window size in packets is above the maximum. To tune this value, in tmsh: `modify sys db dos.tcplowwindowsize value`, where `value` is <=`128`.	Yes
	UDP Flood	udp-flood	UDP flood attack	Yes
Fragmentation	ICMP Fragment	icmp-frag	ICMP fragment flood	Yes
	IPV6 Atomic Fragment	ipv6-atomic-frag	IPv6 Frag header present with M=0 and FragOffset =0	Yes
	IPV6 Fragment Error	ipv6-other-frag	Other IPv6 fragment error	No
	IPv6 Fragment Overlap	ipv6-overlap-frag	IPv6 overlapping fragment error	No
	IPv6 Fragmentat Too Small	ipv6-short-frag	IPv6 short fragment error	Yes
	IP Fragment Error	ip-other-frag	Other IPv4 fragment error	No
	IP Fragment Overlap	ip-overlap-frag	IPv4 overlapping fragment error	No

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
	IP Fragment Too Small	ip-short-frag	IPv4 short fragment error	Yes
Single Endpoint	Single Endpoint Flood	flood	Flood to a single endpoint. You can configure packet types to check for, and packets per second for both detection and rate limiting	No
	Single Endpoint Sweep	sweep	Sweep on a single endpoint. You can configure packet types to check for, and packets per second for both detection and rate limiting	No
SIP	SIP ACK Method	sip-ack-method	SIP ACK packets	No
	SIP BYE Method	sip-bye-method	SIP BYE packets	No
	SIP CANCEL Method	sip-cancel-method	SIP CANCEL packets	No
	SIP INVITE Method	sip-invite-method	SIP INVITE packets	No
	SIP Malformed	sip-malformed	Malformed SIP packets	No
	SIP MESSAGE Method	sip-message-method	SIP MESSAGE packets	No
	SIP NOTIFY Method	sip-notify-method	SIP NOTIFY packets	No
	SIP OPTIONS Method	sip-options-method	SIP OPTIONS packets	No
	SIP OTHER Method	sip-other-method	SIP OTHER packets	No
	SIP PRACK Method	sip-prack-method	SIP PRACK packets	No
	SIP PUBLISH Method	sip-publish-method	SIP PUBLISH packets	No
	SIP REGISTER Method	sip-register-method	SIP REGISTER packets	No
	SIP SUBSCRIBE Method	sip-subscribe-method	SIP SUBSCRIBE packets	No
Other	Host Unreachable	host-unreachable	Host unreachable error	Yes
	LAND Attack	land-attack	Spoofed TCP SYN packet attack	Yes
	TIDCMP	tidcmp	ICMP source quench attack	Yes

Chapter 3

Preventing DoS Sweep and Flood Attacks

- *About DoS sweep and flood attack prevention*
- *Detecting and protecting against single endpoint DoS flood attacks*
- *Detecting and protecting against DoS sweep attacks*
- *Detecting and protecting against UDP flood attacks*
- *Allowing addresses to bypass DoS checks with a whitelist*

About DoS sweep and flood attack prevention

A *sweep attack* is a network scanning technique that typically sweeps your network by sending packets, and using the packet responses to determine live hosts. Typical attacks use ICMP to accomplish this.

The Sweep vector tracks packets by source address. Packets from a specific source that meet the defined single endpoint Sweep criteria, and are above the rate limit, are dropped.

Important: *The sweep mechanism protects against a flood attack from a single source, whether that attack is to a single destination host, or multiple hosts.*

A *flood attack* is a an attack technique that floods your network with packets of a certain type, in an attempt to overwhelm the system. A typical attack might flood the system with SYN packets without then sending corresponding ACK responses. UDP flood attacks flood your network with a large amount of UDP packets, requiring the system to check for applications and send responses.

The Flood vector tracks packets per destination address. Packets to a specific destination that meet the defined Single Endpoint Flood criteria, and are above the rate limit, are dropped.

The BIG-IP® system can detect such attacks with a configurable detection threshold, and can rate limit packets from a source when the detection threshold is reached.

You can configure DoS sweep and flood prevention to detect and prevent floods and sweeps of ICMP, UDP, TCP SYN without ACK, or any IP packets that originate from a single source address, according to the threshold setting. Both IPv4 and IPv6 are supported. The sweep vector acts first, so a packet flood *from a single source address to a single destination address* is handled by the sweep vector.

You can configure DoS sweep and flood prevention through the Device DoS profile.

Detecting and protecting against single endpoint DoS flood attacks

With the DoS Protection Device Configuration screen settings, you can set detection thresholds and rate limits for DoS flood attacks.

1. On the Main tab, click **Security** > **DoS Protection** > **Device Configuration**.
   The DoS Protection Device Configuration screen opens.
2. To log DoS events to a log publisher, from the **Log Publisher** list, select a destination to which the BIG-IP® system sends DoS and DDoS log entries, and click **Update**.
3. In the **Category** column, expand the **Single Endpoint** category.
4. Click **Single Endpoint Flood**.
   The **Single Endpoint Flood** screen opens.
5. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not logged or reported based on this threshold.
6. From the **Default Internal Rate Limit** list, select **Specify** or **Infinite**.

- Use **Specify** to set a value (in packets per second), which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again.
- Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not rate-limited.

7. In the **Packet Type** area, select the packet types you want to detect for this attack type in the **Available** list, and click **<<** to move them to the **Selected** list.
8. Click the **Update** button.
   The flood attack configuration is updated, and the DoS Protection Device Configuration screen opens again.

Now you have configured the system to provide protection against DoS flood attacks, and to allow such attacks to be identified in system logs and reports.

Configure sweep attack prevention, and configure any other DoS responses, in the DoS device configuration. Configure whitelist entries for addresses that you specifically want to bypass all DoS checks. Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system.

Detecting and protecting against DoS sweep attacks

With the DoS Protection Device Configuration screen settings, you can set detection thresholds and rate limits for DoS sweep attacks.

1. On the Main tab, click **Security** > **DoS Protection** > **Device Configuration**.
   The DoS Protection Device Configuration screen opens.
2. To log DoS events to a log publisher, from the **Log Publisher** list, select a destination to which the BIG-IP® system sends DoS and DDoS log entries, and click **Update**.
3. In the **Category** column, expand the **Single Endpoint** category.
4. Click **Single Endpoint Sweep**.
   The Single Endpoint Sweep screen opens.
5. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not logged or reported based on this threshold.
6. From the **Default Internal Rate Limit** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in packets per second), which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not rate-limited.
7. In the **Packet Type** area, select the packet types you want to detect for this attack type in the **Available** list, and click **<<** to move them to the **Selected** list.
8. Click the **Update** button.
   The sweep attack configuration is updated, and the DoS Protection Device Configuration screen opens again.

Now you have configured the system to provide protection against DoS sweep attacks, and to allow such attacks to be identified in system logs and reports.

Configure flood attack prevention, and configure any other DoS responses, in the DoS device configuration. Configure whitelist entries for addresses that you specifically choose to bypass all DoS checks. Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system.

Detecting and protecting against UDP flood attacks

With the DoS Protection Device Configuration screen settings, you can set detection thresholds and rate limits for UDP flood attacks.

1. On the Main tab, click **Security** > **DoS Protection** > **Device Configuration**.
   The DoS Protection Device Configuration screen opens.
2. To log DoS events to a log publisher, from the **Log Publisher** list, select a destination to which the BIG-IP® system sends DoS and DDoS log entries, and click **Update**.
3. In the **Category** column, expand the **Flood** category.
4. Click **UDP Flood**.
   The **UDP Flood** screen opens.
5. From the **Detection Threshold PPS** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in packets per second) for the attack detection threshold. If packets of the specified types cross the threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not logged or reported based on this threshold.
6. From the **Detection Threshold Percent** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in percentage of traffic) for the attack detection threshold. If packets of the specified types cross the percentage threshold, an attack is logged and reported. The system continues to check every second, and marks the threshold as an attack as long as the threshold is exceeded.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not logged or reported based on this threshold.
7. From the **Default Internal Rate Limit** list, select **Specify** or **Infinite**.
   - Use **Specify** to set a value (in packets per second), which cannot be exceeded by packets of this type. All packets of this type over the threshold are dropped. Rate limiting continues until the rate drops below the specified limit again.
   - Use **Infinite** to set no value for the threshold. This specifies that this type of attack is not rate-limited.
8. From the **UDP Port List Type** list, select **Include All Ports** or **Exclude All Ports**.
   An *Include* list checks all the ports you specify in the UDP Port List, using the specified threshold criteria, and ignores all others.
   An *Exclude* list excludes all the ports you specify in the UDP Port List from checking, using the specified threshold criteria, and checks all others. To check all UDP ports, specify an empty exclude list.
9. In the **UDP Port List** area, type a port number to add to an exclude or include UDP port list.
10. In the **UDP Port List** area, select the mode for each port number you want to add to an exclude or include UDP port list.
    - **None** does not include or exclude the port.
    - **Source only** includes or excluded the port from source packets only.
    - **Destination only** includes or excludes the port for destination packets only.
    - **Both Source and Destination** includes or excludes the port in both source and destination packets.

11. Click the **Update** button.
    The UDP Flood attack configuration is updated, and the DoS Protection Device Configuration screen opens again.

Now you have configured the system to provide customized protection against UDP flood attacks, and to allow such attacks to be identified in system logs and reports.

Configure sweep and flood attack prevention, and configure any other DoS responses, in the DoS device configuration screens. Configure whitelist entries for addresses that you specifically choose to bypass all DoS checks. Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system.

Allowing addresses to bypass DoS checks with a whitelist

You can specify whitelist addresses that the DoS profile and DoS Device Configuration do not subject to DoS checks. Whitelist entries are shared between the Dos Protection profile and the DoS Device Configuration.

1. On the Main tab, click **Security** > **DoS Protection** > **White List**.
   The DoS Protection White List screen opens.
2. Click **Create**.
   The New White List Configuration screen opens.
3. In the **Name** field, type a name for the whitelist entry.
4. In the **Description** field, type a description for the whitelist entry.
5. From the **Protocol** list, select the protocol for the whitelist entry.
   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
6. In the **Source** area, specify the IP address and VLAN combination that serves as the source of traffic that the system recognizes as acceptable to pass the DoS checks.
   You can also use **Any** to specify any address or VLAN.
7. For the **Destination** setting, specify the IP address and port combination that serves as the intended destination for traffic that the system recognizes as acceptable to pass DoS checks.
   You can also use **Any** to specify any address or port.
8. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and star a new entry.
   You can add up to eight DoS whitelist entries to the configuration.

You have now configured whitelist addresses that are allowed to bypass DoS checks.

Chapter 4

Detecting and Preventing DNS DoS Attacks

About configuring the BIG-IP system to detect DNS DoS attacks

DNS DoS protection is a type of protocol security. DNS attack detection and prevention serves two functions:

- To detect and automatically drop DNS packets that are malformed or contain errors.
- To log unusual increases in DNS packets of any type, including packets that are malformed, packets that contain errors, or packets of any other type that appear to rapidly increase.

You can use the DNS DoS Protection profile to configure the percentage increase over the system baseline, which indicates that a possible attack is in process on a particular DNS query type, or an increase in anomalous packets. Later, you can use reporting or logging functions to detect such packets, and you can use the DNS Security profile to drop packets with specific query types or header opcodes.

You can define whitelist addresses that the DoS check allows. A whitelist DoS address is passed by the DoS profile, without being subject to the checks in the DoS profile.

DNS DoS protection requires that your virtual server includes a DNS profile, and a DoS profile that includes DNS protocol security.

Task summary

Detecting and protecting against DNS denial-of-service attacks with a DoS profile

You can configure DNS attack settings in a DoS profile that already exists.

The BIG-IP® system handles DNS attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses, by detecting packets per second and increasing packet percentages over time . You can configure settings to identify and rate limit possible DNS attacks with a DoS profile.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click **Create**.
   The Create New DoS Profile screen opens.
3. In the **Profile Name** field, type the name for the profile.
4. To configure DNS security settings, next to **Protocol Security (DNS)**, select **Enabled**.
5. To enable attack detection based on the rate of protocol errors, next to **Protocol Errors Attack Detection**, select **Enabled**.
6. In the **Rate Increased by %** field, type the rate of change in protocol errors to detect as anomalous. The rate of detection compares the average rate over the last minute to the average rate over the last hour. For example, the `500%` base rate would indicate an attack if the average rate for the previous hour was `100000` packets/second, and over the last minute the rate increased to `500000` packets/second.
7. To change the threshold or rate increase for a particular DNS query type, in the DNS Query Attack Detection area, select the **Enabled** check box for each query type that you want to change, then change the values for **Threshold**, **Rate Increase**, and **Rate Limit** in the associated fields.

   For example, to change the thresholds for IPv6 address requests, select the **Enabled** check box next to **aaaa**, then set the threshold for packets per second, the rate increase percentage to be considered an attack, and rate limit in packets per second for such packets.

The Rate Increase compares the average rate over the last minute to the average rate over the last hour. For example, the `500%` base rate would indicate an attack if the average rate for the previous hour was `100000` packets/second, and over the last minute the rate increased to `500000` packets/second.

Note: DNS Query Attack Detection *allows you to configure the thresholds at which the firewall registers an attack. Packets are dropped that exceed the* ***Rate Limit****.*

---

8. Click **Update** to save your changes.

You have now configured a DoS Protection profile to provide custom responses to malformed DNS attacks, and DNS flood attacks, and to allow such attacks to be identified in system logs and reports, and rate limited.

Associate a DNS profile with a virtual server to enable the virtual server to handle DNS traffic. Associate the DoS Protection profile with a virtual server to apply the settings in the profile to traffic on that virtual server. When a DNS attack on a specific query type is detected, you can configure the DNS security profile to drop packets of a query type that appears to be an attack vector.

Creating a custom DNS profile to firewall DNS traffic

Ensure that you have a DNS security profile created before you configure this system DNS profile.

You can create a custom DNS profile to configure the BIG-IP® system firewall traffic through the system.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the General Properties area, from the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. In the DNS Traffic area, from the **DNS Security** list, select **Enabled**.
7. In the DNS Traffic area, from the **DNS Security Profile Name** list, select the name of the DNS firewall profile.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server that handles the DNS traffic that you want to firewall.

Assigning a DNS profile to a virtual server

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. From the **DNS Profile** list, select the profile you want to assign to the virtual server.
5. Click **Update**.

The virtual server now handles DNS traffic.

Associating a DoS profile with a virtual server

You must first create a DoS profile separately, to configure denial-of-service protection for applications, the DNS protocol, or the SIP protocol.

You add denial-of-service protection to a virtual server to provide enhanced protection from DoS attacks, and track anomalous activity on the BIG-IP® system.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. In the **Destination Address** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.
4. From the **Security** menu, choose **Policies**.
5. To enable denial-of-service protection, from the **DoS Protection Profile** list, select **Enabled**, and then, from the **Profile** list, select the DoS profile to associate with the virtual server.
6. Click **Update** to save the changes.

DoS protection is now enabled, and the DoS Protection profile is associated with the virtual server.

Allowing addresses to bypass DoS checks with a whitelist

You can specify whitelist addresses that the DoS profile and DoS Device Configuration do not subject to DoS checks. Whitelist entries are shared between the Dos Protection profile and the DoS Device Configuration.

1. On the Main tab, click **Security** > **DoS Protection** > **White List**.
   The DoS Protection White List screen opens.
2. Click **Create**.
   The New White List Configuration screen opens.
3. In the **Name** field, type a name for the whitelist entry.
4. In the **Description** field, type a description for the whitelist entry.
5. From the **Protocol** list, select the protocol for the whitelist entry.

   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
6. In the **Source** area, specify the IP address and VLAN combination that serves as the source of traffic that the system recognizes as acceptable to pass the DoS checks.

   You can also use **Any** to specify any address or VLAN.
7. For the **Destination** setting, specify the IP address and port combination that serves as the intended destination for traffic that the system recognizes as acceptable to pass DoS checks.

   You can also use **Any** to specify any address or port.
8. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and star a new entry.

   You can add up to eight DoS whitelist entries to the configuration.

You have now configured whitelist addresses that are allowed to bypass DoS checks.

Creating a custom DoS Protection Logging profile

Create a custom Logging profile to log DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.
4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.
5. Click **Finished**.

Assign this custom DoS Protection Logging profile to a virtual server.

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Chapter 5

Detecting SIP DoS Attacks

- *About configuring the BIG-IP system to detect SIP DoS attacks*

About configuring the BIG-IP system to detect SIP DoS attacks

Session Initiation Protocol (SIP) is a signaling protocol that is typically used to control communication sessions such as voice and video calls over IP. On the BIG-IP® system, SIP attack detection detects and automatically drops SIP packets that are malformed or contain errors. In addition, you can use a SIP denial-of-service (DoS) profile to log unusual increases in SIP request packets, including packets that are malformed, packets that contain errors, or packets of any other type that appear to rapidly increase.

You can use the SIP DoS Protection profile to configure the percentage increase over the system baseline that indicates a possible attack is in progress on a particular SIP request type, or an increase in anomalous packets. Later, you can use reporting or logging functions to detect such packets. This is a reporting and tracking function only.

Note: *To use SIP DoS protection, you must create a SIP profile, and attach it to the virtual server to which the SIP DoS feaure is applied.*

Detecting SIP denial-of-service attacks with a DoS profile

In this task, you create the DoS Protection profile and configure SIP settings at the same time. However, you can configure SIP attack detection settings in a DoS profile that already exists.

The BIG-IP® system handles SIP attacks that use malformed packets, protocol errors, and malicious attack vectors. Protocol error attack detection settings detect malformed and malicious packets, or packets that are employed to flood the system with several different types of responses. You can configure settings to identify SIP attacks with a DoS profile.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click **Create**.
   The Create New DoS Profile screen opens.
3. In the **Profile Name** field, type the name for the profile.
4. To configure SIP security settings, next to **Protocol Security (SIP)**, select **Enabled**.
5. To enable attack detection based on the rate of protocol errors, next to **Protocol Errors Attack Detection**, select **Enabled**.
6. In the **Rate threshold** field, type the rate of packets with errors per second to detect as anomalous.
   This threshold sets an absolute limit above which an attack is registered. In addition, you can set individual thresholds for specific request types.
7. In the **Rate Increased by %** field, type the rate of change in protocol errors to detect as anomalous. The rate of detection compares the average rate over the last minute to the average rate over the last hour. For example, the `500%` base rate would indicate an attack if the average rate for the previous hour was `100000` packets/second, and over the last minute the rate increased to `500000` packets/second.
8. To change the threshold or rate increase for a particular SIP request type, in the **SIP Method Attack Detection** settings, select the **Enabled** check box for each request type that you want to change, then change the values for **Threshold** and **Rate Increase** in the associated fields.
   For example, to change the threshold for NOTIFY requests, select the **Enabled** check box next to **notify**, then set the threshold for packets per second and the rate increase percentage to be considered an attack.
   The Rate Increase compares the average rate over the last minute to the average rate over the last hour. For example, the `500%` base rate would indicate an attack if the average rate for the previous hour was `100000` packets/second, and over the last minute the rate increased to `500000` packets/second.

Note: *SIP request detection allows you to configure the thresholds at which the firewall registers an attack. However, no packets are dropped if an attack is detected.*

9. Click **Update** to save your changes.

You have now configured a DoS Protection profile to provide custom responses to malformed SIP attacks, and SIP flood attacks, and to allow such attacks to be identified in system logs and reports.

Associate the DoS Protection profile with a virtual server to apply the settings in the profile to traffic on that virtual server. When a SIP attack on a specific query type is detected, you can be alerted with various system monitors.

Assigning a SIP profile to a virtual server

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. From the **SIP Profile** list, select the name of the SIP profile that you previously created.
5. Click **Update**.

The virtual server now uses the SIP settings from the SIP profile.

Associating a DoS profile with a virtual server

You must first create a DoS profile separately, to configure denial-of-service protection for applications, the DNS protocol, or the SIP protocol.

You add denial-of-service protection to a virtual server to provide enhanced protection from DoS attacks, and track anomalous activity on the BIG-IP® system.

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. In the **Destination Address** field, type the IP address in CIDR format.

   The supported format is address/prefix, where the prefix length is in bits. For example, an IPv4 address/prefix is `10.0.0.1` or `10.0.0.0/24`, and an IPv6 address/prefix is `ffe1::0020/64` or `2001:ed8:77b5:2:10:10:100:42/64`. When you use an IPv4 address without specifying a prefix, the BIG-IP® system automatically uses a `/32` prefix.
4. From the **Security** menu, choose **Policies**.
5. To enable denial-of-service protection, from the **DoS Protection Profile** list, select **Enabled**, and then, from the **Profile** list, select the DoS profile to associate with the virtual server.
6. Click **Update** to save the changes.

DoS protection is now enabled, and the DoS Protection profile is associated with the virtual server.

Allowing addresses to bypass DoS checks with a whitelist

You can specify whitelist addresses that the DoS profile and DoS Device Configuration do not subject to DoS checks. Whitelist entries are shared between the Dos Protection profile and the DoS Device Configuration.

1. On the Main tab, click **Security** > **DoS Protection** > **White List**.
   The DoS Protection White List screen opens.
2. Click **Create**.
   The New White List Configuration screen opens.
3. In the **Name** field, type a name for the whitelist entry.
4. In the **Description** field, type a description for the whitelist entry.
5. From the **Protocol** list, select the protocol for the whitelist entry.
   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
6. In the **Source** area, specify the IP address and VLAN combination that serves as the source of traffic that the system recognizes as acceptable to pass the DoS checks.
   You can also use **Any** to specify any address or VLAN.
7. For the **Destination** setting, specify the IP address and port combination that serves as the intended destination for traffic that the system recognizes as acceptable to pass DoS checks.
   You can also use **Any** to specify any address or port.
8. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and star a new entry.
   You can add up to eight DoS whitelist entries to the configuration.

You have now configured whitelist addresses that are allowed to bypass DoS checks.

Creating a custom SIP DoS Protection Logging profile

Create a custom Logging profile to log SIP DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.
4. In the SIP DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log SIP DoS events.
   You can specify publishers for other DoS types in the same profile, for example, for DNS or Application DoS Protection.
5. Click **Finished**.

Assign this custom SIP DoS Protection Logging profile to a virtual server.

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Chapter 6

SNMP Trap Configuration

Overview: SNMP trap configuration

SNMP *traps* are definitions of unsolicited notification messages that the BIG-IP® alert system and the SNMP agent send to the SNMP manager when certain events occur on the BIG-IP system. Configuring SNMP traps on a BIG-IP system means configuring how the BIG-IP system handles traps, as well as setting the destination to which the notifications are sent.

The BIG-IP system stores SNMP traps in two specific files:

`/etc/alertd/alert.conf`
Contains default SNMP traps.

Important: *Do not add or remove traps from the `/etc/alertd/alert.conf` file.*

`/config/user_alert.conf`
Contains user-defined SNMP traps.

Task summary

Perform these tasks to configure SNMP traps for certain events and set trap destinations.

Enabling traps for specific events
Setting v1 and v2c trap destinations
Setting v3 trap destinations
Viewing pre-configured SNMP traps
Creating custom SNMP traps

Enabling traps for specific events

You can configure the SNMP agent on the BIG-IP® system to send, or refrain from sending, notifications to the traps destinations.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Configuration**.
2. To send traps when an administrator starts or stops the SNMP agent, verify that the **Enabled** check box for the **Agent Start/Stop** setting is selected.
3. To send notifications when authentication warnings occur, select the **Enabled** check box for the **Agent Authentication** setting.
4. To send notifications when certain warnings occur, verify that the **Enabled** check box for the **Device** setting is selected.
5. Click **Update**.

The BIG-IP system automatically updates the `alert.conf` file.

Setting v1 and v2c trap destinations

Specify the IP address of the SNMP manager in order for the BIG-IP® system to send notifications.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Destination**.
2. Click **Create**.

3. For the **Version** setting, select either `v1` or `v2c`.
4. In the **Community** field, type the community name for the SNMP agent running on the BIG-IP system.
5. In the **Destination** field, type the IP address of the SNMP manager.
6. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
7. Click **Finished**.

Setting v3 trap destinations

Specify the destination SNMP manager to which the BIG-IP® system sends notifications.

1. On the Main tab, click **System** > **SNMP** > **Traps** > **Destination**.
2. Click **Create**.
3. For the **Version** setting, select `v3`.
4. In the **Destination** field, type the IP address of the SNMP manager.
5. In the **Port** field, type the port number on the SNMP manager that is assigned to receive the traps.
6. From the **Security Level** list, select the level of security at which you want SNMP messages processed.

Option	Description
Auth, No Privacy	Process SNMP messages using authentication but without encryption. When you use this value, you must also provide values for the **Security Name**, **Authentication Protocol**, and **Authentication Password** settings.
Auth and Privacy	Process SNMP messages using authentication and encryption. When you use this value, you must also provide values for the **Security Name**, **Authentication Protocol**, **Authentication Password**, **Privacy Protocol**, and **Privacy Password** settings.

7. In the **Security Name** field, type the user name the system uses to handle SNMP v3 traps.
8. In the **Engine ID** field, type an administratively unique identifier for an SNMP engine. (This setting is optional.) You can find the engine ID in the `/config/net-snmp/snmpd.conf` file on the BIG-IP system. Please note that this ID is identified in the file as the value of the oldEngineID token.
9. From the **Authentication Protocol** list, select the algorithm the system uses to authenticate SNMP v3 traps.

   When you set this value, you must also enter a value in the **Authentication Password** field.
10. In the **Authentication Password** field, type the password the system uses to handle an SNMP v3 trap.

    When you set this value, you must also select a value from the **Authentication Protocol** list.

    Note: *The authentication password must be at least 8 characters long.*
11. If you selected **Auth and Privacy** from the **Security Level** list, from the **Privacy Protocol** list, select the algorithm the system uses to encrypt SNMP v3 traps. When you set this value, you must also enter a value in the **Privacy Password** field.
12. If you selected **Auth and Privacy** from the **Security Level** list, in the **Privacy Password** field, type the password the system uses to handle an encrypted SNMP v3 trap. When you set this value, you must also select a value from the **Privacy Protocol** list.

    Note: *The authentication password must be at least 8 characters long.*
13. Click **Finished**.

Viewing pre-configured SNMP traps

Verify that your user account grants you access to the advanced shell.

Pre-configured traps are stored in the `/etc/alertd/alert.conf` file. View these SNMP traps to understand the data that the SNMP manager can use.

Use this command to view the SNMP traps that are pre-configured on the BIG-IP® system: `cat /etc/alertd/alert.conf`.

Creating custom SNMP traps

Verify that your user account grants you access to tmsh.

Create custom SNMP traps that alert the SNMP manager to specific SNMP events that occur on the network when the pre-configured traps do not meet all of your needs.

1. Log in to the command line.
2. Create a backup copy of the file `/config/user_alert.conf`, by typing this command: `cp /config/user_alert.conf` *`backup_file_name`*
   For example, type: `cp /config/user_alert.conf /config/user_alert.conf.backup`
3. With a text editor, open the file `/config/user_alert.conf`.
4. Add a new SNMP trap.
   The required format is:

```
alert alert_name "matched message" {
    snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.XXX"
   }
```

- *`alert_name`* represents a descriptive name. The *`alert_name`* or *`matched_message`* value cannot match the corresponding value in any of the SNMP traps defined in the `/etc/alertd/alert.conf` or `/config/user_alert.conf` file.
- *`matched_message`* represents the text that matches the Syslog message that triggers the custom trap. You can specify either a portion of the Syslog message text or use a regular expression. Do not include the Syslog prefix information, such as the date stamp and process ID, in the match string.
- The *`XXX`* portion of the OID value represents a number that is unique to this OID. Specify any OID that meets all of these criteria:
  - Is in standard OID format and within the range `.1.3.6.1.4.1.3375.2.4.0.300` through `.1.3.6.1.4.1.3375.2.4.0.999`.
  - Is in a numeric range that can be processed by your trap receiving tool.
  - Does not exist in the MIB file `/usr/share/snmp/mibs/F5-BIGIP-COMMON-MIB.txt`.
  - Is not used in another custom trap.

As an example, to create a custom SNMP trap that is triggered whenever the system logs switchboard failsafe status changes, add the following trap definition to `/config/user_alert.conf`.

```
alert SWITCHBOARD_FAILSAFE_STATUS "Switchboard Failsafe (.*)" {
         snmptrap OID=".1.3.6.1.4.1.3375.2.4.0.500"
    }
```

This trap definition causes the system to log the following message to the file `/var/log/ltm`, when switchboard failsafe is enabled: `Sep 23 11:51:40 bigip1.askf5.com lacpd[27753]: 01160016:6: Switchboard Failsafe enabled`.

5. Save the file.
6. Close the text editor.
7. Restart the `alertd` daemon by typing this command: `bigstart restart alertd`

   If the `alertd` daemon fails to start, examine the newly-added trap entry to ensure that the format is correct.

Chapter 7

Configuring High-Speed Remote Logging of DoS Events

Overview: Configuring DoS Protection event logging

You can configure the BIG-IP® system to log information about BIG-IP system denial-of-service (DoS) events, and send the log messages to remote high-speed log servers.

Important: *The BIG-IP Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure DoS Protection event logging. Additionally, for high-volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.*

When configuring remote high-speed logging of DoS Protection event logging, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging of DoS Protection events.

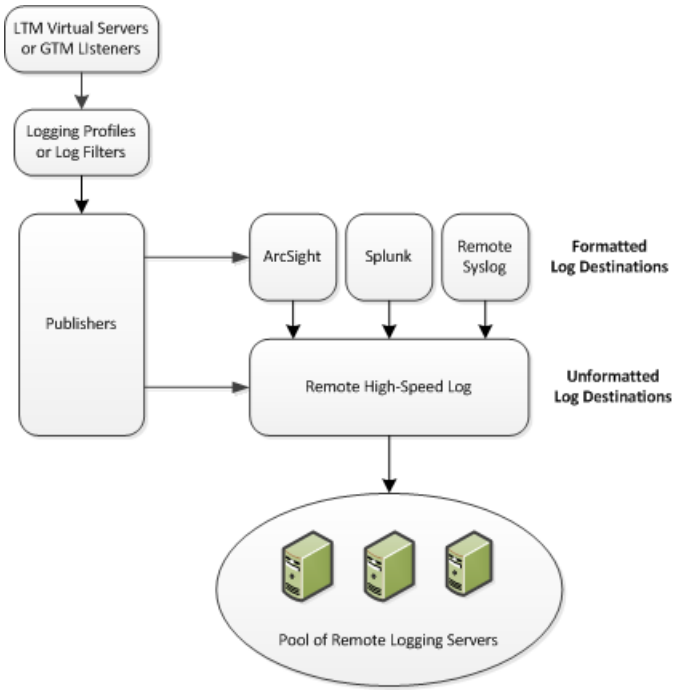

Figure 1: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure logging of DoS Protection events on the BIG-IP® system.

Note: *Enabling logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom DoS Protection Logging profile
Configuring an LTM virtual server for DoS Protection event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom DoS Protection Logging profile

Create a custom Logging profile to log DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.

4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.

5. Click **Finished**.

Assign this custom DoS Protection Logging profile to a virtual server.

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific DoS Protection events and sends the logs to a specific location.

Chapter 8

Configuring High-Speed Remote Logging of DNS DoS Events

Overview: Configuring DNS DoS Protection event logging

You can configure the BIG-IP® system to log information about BIG-IP system DNS denial-of-service (DoS) events, and send the log messages to remote high-speed log servers.

Important: *The BIG-IP Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure DNS DoS Protection event logging. Additionally, for high volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.*

When configuring remote high-speed logging of DNS DoS Protection event logging, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging of DoS Protection events.

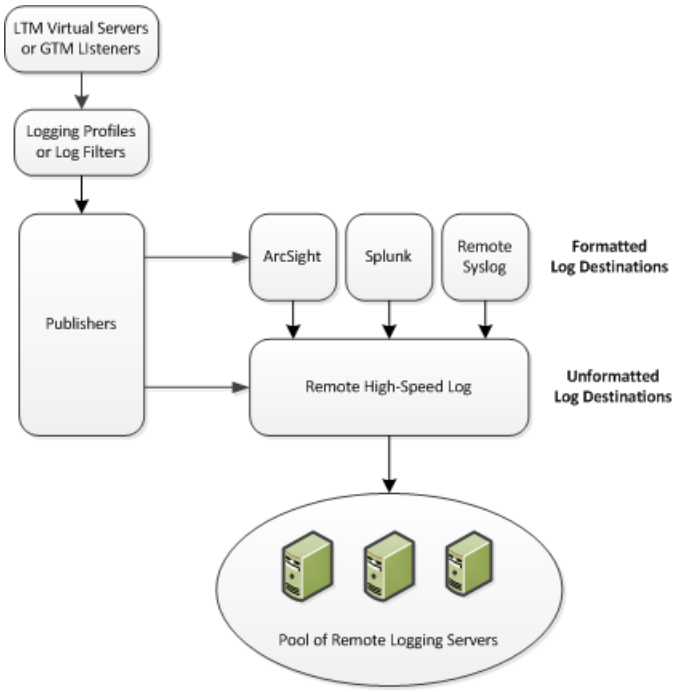

Figure 2: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure logging of DNS DoS Protection events on the BIG-IP® system.

Note: *Enabling logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom DNS DoS Protection Logging profile
Configuring an LTM virtual server for DoS Protection event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

The Pool List screen opens.

2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.

2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom DNS DoS Protection Logging profile

Create a custom Logging profile to log DNS DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.

The New Logging Profile screen opens.

3. Select the **DoS Protection** check box.
4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.
5. Click **Finished**.

Assign this custom DNS DoS Protection Logging profile to a virtual server.

Overview: Configuring IPFIX logging for DNS DoS
Creating a publisher
Overview: Configuring IPFIX logging for SIP DoS
Creating a publisher

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific DoS Protection events and sends the logs to a specific location.

Chapter 9

About Logging DNS DoS Events to IPFIX Collectors

Overview: Configuring IPFIX logging for DNS DoS

You can configure the BIG-IP® system to log information about DNS denial-of-service (DoS) events and send the log messages to remote IPFIX collectors.

IPFIX is a set of IETF standards. The BIG-IP system supports logging of DNS DoS events over the IPFIX protocol. IPFIX logs are raw, binary-encoded strings with their fields and field lengths defined by IPFIX templates. *IPFIX collectors* are external devices that can receive IPFIX templates and use them to interpret IPFIX logs.

The configuration process involves creating and connecting the following configuration objects:

Object	Reason
Pool of IPFIX collectors	Create a pool of IPFIX collectors to which the BIG-IP system can send IPFIX log messages.
Destination	Create a log destination to format the logs in IPFIX templates, and forward the logs to the IPFIX collectors.
Publisher	Create a log publisher to send logs to a set of specified log destinations.

Task summary

Perform these tasks to configure IPFIX logging of DNS DoS events on the BIG-IP system.

Note: *Enabling IPFIX logging impacts BIG-IP system performance.*

Assembling a pool of IPFIX collectors
Creating an IPFIX log destination
Creating a publisher
Creating a custom DNS DoS Protection Logging profile

Assembling a pool of IPFIX collectors

Before creating a pool of IPFIX collectors, gather the IP addresses of the collectors that you want to include in the pool. Ensure that the remote IPFIX collectors are configured to listen to and receive log messages from the BIG-IP® system.

These are the steps for creating a pool of IPFIX collectors. The BIG-IP system can send IPFIX log messages to this pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each IPFIX collector that you want to include in the pool:
   a) Type the collector's IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a port number in the **Service Port** field.

By default, IPFIX collectors listen on UDP or TCP port `4739` and Netflow V9 devices listen on port `2055`, though the port is configurable at each collector.

c) Click **Add**.

5. Click **Finished**.

Creating an IPFIX log destination

A log destination of the **IPFIX** type specifies that log messages are sent to a pool of IPFIX collectors. Use these steps to create a log destination for IPFIX collectors.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **IPFIX**.
5. From the **Protocol** list, select **IPFIX** or **Netflow V9**, depending on the type of collectors you have in the pool.
6. From the **Pool Name** list, select an LTM® pool of IPFIX collectors.
7. From the **Transport Profile** list, select **TCP**, **UDP**, or any customized profile derived from TCP or UDP.
8. The **Template Retransmit Interval** is the time between transmissions of IPFIX templates to the pool of collectors. The BIG-IP system only retransmits its templates if the **Transport Profile** is a **UDP** profile.

   An *IPFIX template* defines the field types and byte lengths of the binary IPFIX log messages. The logging destination sends the template for a given log type (for example, NAT44 logs or customized logs from an iRule) before sending any of those logs, so that the IPFIX collector can read the logs of that type. The logging destination assigns a template ID to each template, and places the template ID into each log that uses that template.

   The log destination periodically retransmits all of its IPFIX templates over a UDP connection. The retransmissions are helpful for UDP connections, which are lossy.
9. The **Template Delete Delay** is the time that the BIG-IP device should pause between deleting an obsolete template and re-using its template ID. This feature is helpful for systems that can create custom IPFIX templates with iRules.
10. The **Server SSL Profile** applies Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TCP connections. You can only choose an SSL profile if the **Transport Profile** is a **TCP** profile. Choose an SSL profile that is appropriate for the IPFIX collectors' SSL/TLS configuration.

    SSL or TLS requires extra processing and therefore slows the connection, so we only recommend this for sites where the connections to the IPFIX collectors have a potential security risk.
11. Click **Finished**.

Creating a publisher

A publisher specifies where the BIG-IP® system sends log messages for IPFIX logs.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.

3. In the **Name** field, type a unique, identifiable name for this publisher.
4. Use the Log Destinations area to select an existing IPFIX destination (perhaps along with other destinations for your logs): click any destination name in the **Available** list, and click **<<** to move it to the **Selected** list.
5. Click **Finished**.

Creating a custom DNS DoS Protection Logging profile

Create a custom Logging profile to log DNS DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.
4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.
5. Click **Finished**.

Assign this custom DNS DoS Protection Logging profile to a virtual server.

Overview: Configuring IPFIX logging for DNS DoS

Creating a publisher

Overview: Configuring IPFIX logging for SIP DoS

Creating a publisher

Implementation result

Now you have an implementation in which the BIG-IP® system logs messages about DNS DoS events and sends the log messages to a pool of IPFIX collectors.

Chapter 10

Filtering DNS Packets

About DNS protocol filtering

With a DNS security profile, you can filter DNS to allow or deny specific DNS query types, and to deny specific DNS opcodes. The DNS security profile is attached to, and works with, a local traffic DNS profile to configure a range of DNS settings for a virtual server. Use DNS protocol filtering:

- To filter DNS query types or header opcodes that are not necessary or relevant in your configuration, or that you do not want your DNS servers to handle.
- As a remediation tool to drop packets of a specific query type, if a DoS Protection Profile identifies anomalous DNS activity with that query type.

Filtering DNS traffic with a DNS security profile
Creating a custom DNS profile to firewall DNS traffic

Filtering DNS traffic with a DNS security profile

In this task, you create a DNS security profile and configure DNS security settings at the same time. However, you can also configure settings in a DNS security profile that already exists.

The BIG-IP® system can allow or drop packets of specific DNS query types, or with specific opcodes, to prevent attacks or allow legitimate DNS traffic. Use this to filter out header opcodes or query types that are not necessary on your system, or to respond to suspicious increases in packets of a certain type, as identified with the DNS security profile.

1. On the Main tab, click **Security** > **Protocol Security** > **Security Profiles** > **DNS**.
   The DNS Security Profiles list screen opens.
2. Click **Create**.
   The Create New DoS Profile screen opens.
3. In the **Profile Name** field, type the name for the profile.
4. From the **Query Type** list, select how to handle query types you add to the **Active** list.
   - Select **Inclusion** to allow packets with the DNS query types you add to the **Active** list, and drop all others.
   - Select **Exclusion** to deny packets with the DNS query types you add to the **Active** list, and allow all others.
5. In the **Profile Name** field, type the name for the profile.
6. In the **Profile Name** field, type the name for the profile.
7. In the **Profile Name** field, type the name for the profile.
8. Click **Update** to save your changes.

Now you have configured the profile to include or exclude only specified DNS query types and header opcodes.

Specify this DNS security profile in a local traffic DNS profile attached to a virtual server.

Creating a custom DNS profile to firewall DNS traffic

Ensure that you have a DNS security profile created before you configure this system DNS profile.

You can create a custom DNS profile to configure the BIG-IP® system firewall traffic through the system.

1. On the Main tab, click **Local Traffic** > **Profiles** > **Services** > **DNS**.
   The DNS profile list screen opens.
2. Click **Create**.
   The New DNS Profile screen opens.
3. In the **Name** field, type a unique name for the profile.
4. In the General Properties area, from the **Parent Profile** list, accept the default **dns** profile.
5. Select the **Custom** check box.
6. In the DNS Traffic area, from the **DNS Security** list, select **Enabled**.
7. In the DNS Traffic area, from the **DNS Security Profile Name** list, select the name of the DNS firewall profile.
8. Click **Finished**.

Assign the custom DNS profile to the virtual server that handles the DNS traffic that you want to firewall.

Assigning a DNS profile to a virtual server

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. From the **Configuration** list, select **Advanced**.
4. From the **DNS Profile** list, select the profile you want to assign to the virtual server.
5. Click **Update**.

The virtual server now handles DNS traffic.

Chapter 11

Configuring High-Speed Remote Logging of SIP DoS Events

Overview: Configuring SIP DoS Protection event logging

You can configure the BIG-IP® system to log information about BIG-IP system SIP protocol denial-of-service (DoS) events, and send the log messages to remote high-speed log servers.

Important: *The Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure SIP DoS Protection event logging. Additionally, for high volume logging requirements, such as DoS, ensure that the BIG-IP system sends the event logs to a remote log server.*

When configuring remote high-speed logging of DoS Protection event logging, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging of DoS Protection events.

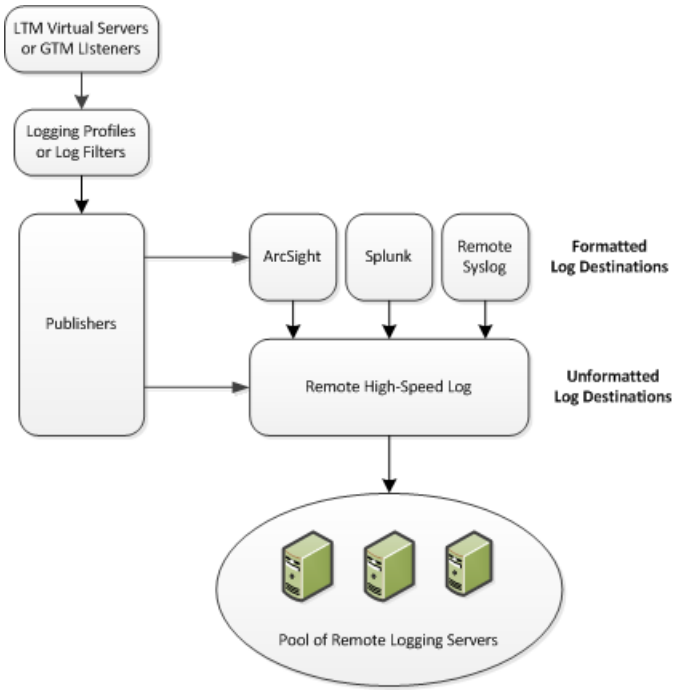

Figure 3: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure logging of SIP DoS Protection events on the BIG-IP® system.

Note: *Enabling logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom SIP DoS Protection Logging profile
Configuring an LTM virtual server for DoS Protection event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

The Pool List screen opens.

2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.

2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom SIP DoS Protection Logging profile

Create a custom Logging profile to log SIP DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.

The New Logging Profile screen opens.

3. Select the **DoS Protection** check box.
4. In the SIP DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log SIP DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for DNS or Application DoS Protection.
5. Click **Finished**.

Assign this custom SIP DoS Protection Logging profile to a virtual server.

Configuring an LTM virtual server for DoS Protection event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom DoS Protection Logging profile to a virtual server when you want the BIG-IP system to log DoS Protection events on the traffic the virtual server processes.

Note: *This task applies only to LTM®-provisioned systems.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

---

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific DoS Protection events and sends the logs to a specific location.

Chapter 12

About Logging SIP DoS Events to IPFIX Collectors

Overview: Configuring IPFIX logging for SIP DoS

You can configure the BIG-IP® system to log information about SIP denial-of-service (SIP DoS) events and send the log messages to remote IPFIX collectors.

IPFIX is a set of IETF standards. The BIG-IP system supports logging of SIP DoS events over the IPFIX protocol . IPFIX logs are raw, binary-encoded strings with their fields and field lengths defined by IPFIX templates. *IPFIX collectors* are external devices that can receive IPFIX templates and use them to interpret IPFIX logs.

The configuration process involves creating and connecting the following configuration objects:

Object	Reason
Pool of IPFIX collectors	Create a pool of IPFIX collectors to which the BIG-IP system can send IPFIX log messages.
Destination	Create a log destination to format the logs in IPFIX templates, and forward the logs to the IPFIX collectors.
Publisher	Create a log publisher to send logs to a set of specified log destinations.

Task summary

Perform these tasks to configure IPFIX logging of SIP DoS events on the BIG-IP system.

Note: *Enabling IPFIX logging impacts BIG-IP system performance.*

Assembling a pool of IPFIX collectors
Creating an IPFIX log destination
Creating a publisher
Creating a custom DNS DoS Protection Logging profile

Assembling a pool of IPFIX collectors

Before creating a pool of IPFIX collectors, gather the IP addresses of the collectors that you want to include in the pool. Ensure that the remote IPFIX collectors are configured to listen to and receive log messages from the BIG-IP® system.

These are the steps for creating a pool of IPFIX collectors. The BIG-IP system can send IPFIX log messages to this pool.

1. On the Main tab, click **Local Traffic** > **Pools**.
   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.
3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each IPFIX collector that you want to include in the pool:
   a) Type the collector's IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a port number in the **Service Port** field.

By default, IPFIX collectors listen on UDP or TCP port `4739` and Netflow V9 devices listen on port `2055`, though the port is configurable at each collector.

c) Click **Add**.

5. Click **Finished**.

Creating an IPFIX log destination

A log destination of the **IPFIX** type specifies that log messages are sent to a pool of IPFIX collectors. Use these steps to create a log destination for IPFIX collectors.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **IPFIX**.
5. From the **Protocol** list, select **IPFIX** or **Netflow V9**, depending on the type of collectors you have in the pool.
6. From the **Pool Name** list, select an LTM® pool of IPFIX collectors.
7. From the **Transport Profile** list, select **TCP**, **UDP**, or any customized profile derived from TCP or UDP.
8. The **Template Retransmit Interval** is the time between transmissions of IPFIX templates to the pool of collectors. The BIG-IP system only retransmits its templates if the **Transport Profile** is a **UDP** profile.

   An *IPFIX template* defines the field types and byte lengths of the binary IPFIX log messages. The logging destination sends the template for a given log type (for example, NAT44 logs or customized logs from an iRule) before sending any of those logs, so that the IPFIX collector can read the logs of that type. The logging destination assigns a template ID to each template, and places the template ID into each log that uses that template.

   The log destination periodically retransmits all of its IPFIX templates over a UDP connection. The retransmissions are helpful for UDP connections, which are lossy.
9. The **Template Delete Delay** is the time that the BIG-IP device should pause between deleting an obsolete template and re-using its template ID. This feature is helpful for systems that can create custom IPFIX templates with iRules.
10. The **Server SSL Profile** applies Secure Socket Layer (SSL) or Transport Layer Security (TLS) to TCP connections. You can only choose an SSL profile if the **Transport Profile** is a **TCP** profile. Choose an SSL profile that is appropriate for the IPFIX collectors' SSL/TLS configuration.

    SSL or TLS requires extra processing and therefore slows the connection, so we only recommend this for sites where the connections to the IPFIX collectors have a potential security risk.
11. Click **Finished**.

Creating a publisher

A publisher specifies where the BIG-IP® system sends log messages for IPFIX logs.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.

3. In the **Name** field, type a unique, identifiable name for this publisher.
4. Use the Log Destinations area to select an existing IPFIX destination (perhaps along with other destinations for your logs): click any destination name in the **Available** list, and click **<<** to move it to the **Selected** list.
5. Click **Finished**.

Creating a custom DNS DoS Protection Logging profile

Create a custom Logging profile to log DNS DoS Protection events and send the log messages to a specific location.

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.
2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **DoS Protection** check box.
4. In the DNS DoS Protection area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS DoS events.

   You can specify publishers for other DoS types in the same profile, for example, for SIP or Application DoS Protection.
5. Click **Finished**.

Assign this custom DNS DoS Protection Logging profile to a virtual server.

Overview: Configuring IPFIX logging for DNS DoS

Creating a publisher

Overview: Configuring IPFIX logging for SIP DoS

Creating a publisher

Implementation result

Now you have an implementation in which the BIG-IP® system logs messages about SIP DoS events and sends the log messages to a pool of IPFIX collectors.

Chapter 13

Configuring High-Speed Remote Logging of Protocol Security Events

Overview: Configuring Remote Protocol Security Event Logging

You can configure the BIG-IP® system to log information about BIG-IP system Protocol Security events and send the log messages to remote high-speed log servers.

Important: *The Advanced Firewall Manager™ (AFM™) must be licensed and provisioned before you can configure Protocol Security event logging.*

When configuring remote high-speed logging of Protocol Security events, it is helpful to understand the objects you need to create and why, as described here:

Object	Reason
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP system can send log messages.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.
Destination (formatted)	If your remote log servers are the ArcSight, Splunk, IPFIX, or Remote Syslog type, create an additional log destination to format the logs in the required format and forward the logs to a remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.
Logging profile	Create a custom Logging profile to enable logging of user-specified data at a user-specified level, and associate a log publisher with the profile.
LTM® virtual server	Associate a custom Logging profile with a virtual server to define how the BIG-IP system logs security events on the traffic that the virtual server processes.

This illustration shows the association of the configuration objects for remote high-speed logging.

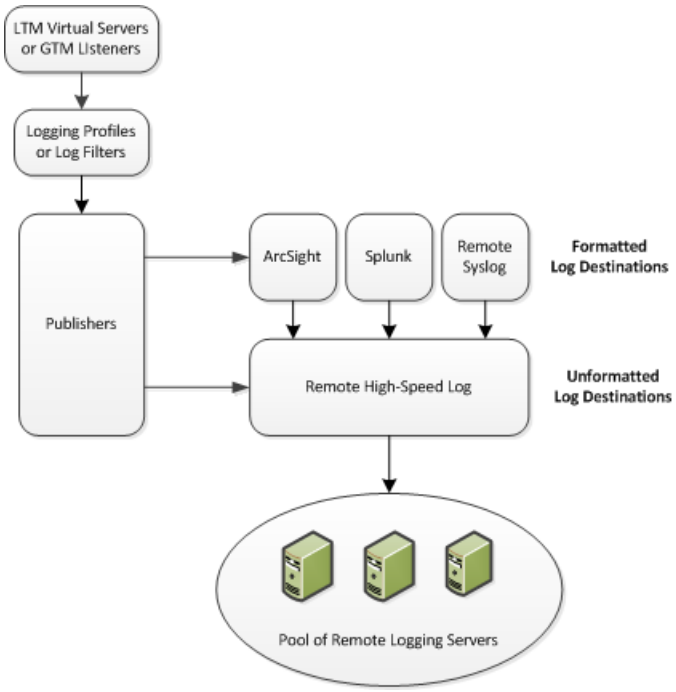

Figure 4: Association of remote high-speed logging configuration objects

Task summary

Perform these tasks to configure Protocol Security event logging on the BIG-IP® system.

Note: *Enabling remote high-speed logging impacts BIG-IP system performance.*

Creating a pool of remote logging servers
Creating a remote high-speed log destination
Creating a formatted remote high-speed log destination
Creating a publisher
Creating a custom Protocol Security Logging profile
Configuring a virtual server for Protocol Security event logging
Disabling logging

Creating a pool of remote logging servers

Before creating a pool of log servers, gather the IP addresses of the servers that you want to include in the pool. Ensure that the remote log servers are configured to listen to and receive log messages from the BIG-IP® system.

Create a pool of remote log servers to which the BIG-IP system can send log messages.

1. On the Main tab, click the applicable path.
   - **DNS** > **Delivery** > **Load Balancing** > **Pools**
   - **Local Traffic** > **Pools**

   The Pool List screen opens.
2. Click **Create**.
   The New Pool screen opens.

3. In the **Name** field, type a unique name for the pool.
4. Using the **New Members** setting, add the IP address for each remote logging server that you want to include in the pool:
   a) Type an IP address in the **Address** field, or select a node address from the **Node List**.
   b) Type a service number in the **Service Port** field, or select a service name from the list.

   Note: *Typical remote logging servers require port* `514`*.*

   c) Click **Add**.
5. Click **Finished**.

Creating a remote high-speed log destination

Before creating a remote high-speed log destination, ensure that at least one pool of remote log servers exists on the BIG-IP® system.

Create a log destination of the **Remote High-Speed Log** type to specify that log messages are sent to a pool of remote log servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.
4. From the **Type** list, select **Remote High-Speed Log**.

   Important: *If you use log servers such as Remote Syslog, Splunk, or ArcSight, which require data be sent to the servers in a specific format, you must create an additional log destination of the required type, and associate it with a log destination of the* ***Remote High-Speed Log*** *type. With this configuration, the BIG-IP system can send data to the servers in the required format.*

   The BIG-IP system is configured to send an unformatted string of text to the log servers.
5. From the **Pool Name** list, select the pool of remote log servers to which you want the BIG-IP system to send log messages.
6. From the **Protocol** list, select the protocol used by the high-speed logging pool members.
7. Click **Finished**.

Creating a formatted remote high-speed log destination

Ensure that at least one remote high-speed log destination exists on the BIG-IP® system.

Create a formatted logging destination to specify that log messages are sent to a pool of remote log servers, such as Remote Syslog, Splunk, or ArcSight servers.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Destinations**.
   The Log Destinations screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this destination.

4. From the **Type** list, select a formatted logging destination, such as **IPFIX**, **Remote Syslog**, **Splunk**, or **ArcSight**.

   Important: *ArcSight formatting is only available for logs coming from Advanced Firewall Manager (AFM), Application Security Manager™ (ASM), and the Secure Web Gateway component of Access Policy Manager® (APM®). IPFIX is not available for Secure Web Gateway. Remote Syslog formatting is the only type supported for logs coming from APM. The Splunk format is a predefined format of key value pairs.*

   The BIG-IP system is configured to send a formatted string of text to the log servers.
5. If you selected **Remote Syslog**, from the **Syslog Format** list, select a format for the logs, and then from the **High-Speed Log Destination** list, select the destination that points to a pool of remote Syslog servers to which you want the BIG-IP system to send log messages.

   Important: *For logs coming from Access Policy Manager® (APM®), only the BSD Syslog format is supported.*

6. If you selected **Splunk** or **IPFIX**, from the **Forward To** list, select the destination that points to a pool of high-speed log servers to which you want the BIG-IP system to send log messages.
7. Click **Finished**.

Creating a publisher

Ensure that at least one destination associated with a pool of remote log servers exists on the BIG-IP® system.

Create a publisher to specify where the BIG-IP system sends log messages for specific resources.

1. On the Main tab, click **System** > **Logs** > **Configuration** > **Log Publishers**.
   The Log Publishers screen opens.
2. Click **Create**.
3. In the **Name** field, type a unique, identifiable name for this publisher.
4. For the **Destinations** setting, select a destination from the **Available** list, and click **<<** to move the destination to the **Selected** list.

   Note: *If you are using a formatted destination, select the destination that matches your log servers, such as Remote Syslog, Splunk, or ArcSight.*

5. Click **Finished**.

Creating a custom Protocol Security Logging profile

Create a logging profile to log Protocol Security events for the traffic handled by the virtual server to which the profile is assigned.

Note: *You can configure logging profiles for HTTP and DNS security events on Advanced Firewall Manager™, and FTP and SMTP security events on Application Security Manager™.*

1. On the Main tab, click **Security** > **Event Logs** > **Logging Profiles**.
   The Logging Profiles list screen opens.

2. Click **Create**.
   The New Logging Profile screen opens.
3. Select the **Protocol Security** check box, to enable the BIG-IP system to log HTTP, FTP, DNS, and SMTP protocol request events.
4. In the HTTP, FTP, and SMTP Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log HTTP, FTP, and SMTP Security events.
5. In the DNS Security area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log DNS Security events.
6. Select the **Log Dropped DNS Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
7. Select the **Log Filtered Dropped DNS Requests** check box, to enable the BIG-IP system to log DNS requests dropped due to DNS query/header-opcode filtering.

   Note: *The system does not log DNS requests that are dropped due to errors in the way the system processes DNS packets.*

8. Select the **Log Malformed DNS Requests** check box, to enable the BIG-IP system to log malformed DNS requests.
9. Select the **Log Rejected DNS Requests** check box, to enable the BIG-IP system to log rejected DNS requests.
10. Select the **Log Malicious DNS Requests** check box, to enable the BIG-IP system to log malicious DNS requests.
11. From the **Storage Format** list, select how the BIG-IP system formats the log. Your choices are:

Option	Description
None	Specifies the default format type in which the BIG-IP system logs messages to a remote Syslog server, for example: `"management_ip_address","bigip_hostname","context_type", "context_name","src_ip","dest_ip","src_port", "dest_port","vlan","protocol","route_domain", "acl_rule_name","action","drop_reason`
Field-List	This option allows you to: • Select from a list, the fields to be included in the log. • Specify the order the fields display in the log. • Specify the delimiter that separates the content in the log. The default delimiter is the comma character.
User-Defined	This option allows you to: • Select from a list, the fields to be included in the log. • Cut and paste, in a string of text, the order the fields display in the log.

12. Click **Finished**.

Assign this custom Protocol Security Logging profile to a virtual server.

Configuring a virtual server for Protocol Security event logging

Ensure that at least one Log Publisher exists on the BIG-IP® system.

Assign a custom Protocol Security Logging profile to a virtual server when you want the BIG-IP system to log Protocol Security events on the traffic the virtual server processes.

Note: *This task applies only to systems provisioned at a minimum level (or higher) for* ***Local Traffic (LTM)****. You can check the provisioning level on the* ***System*** *>* ***Resource Provisioning*** *screen.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Enabled**. Then, for the **Profile** setting, move the profiles that log specific events to specific locations from the **Available** list to the **Selected** list.
5. Click **Update** to save the changes.

Disabling logging

Disable Network Firewall, Protocol Security, or DoS Protection event logging when you no longer want the BIG-IP® system to log specific events on the traffic handled by specific resources.

Note: *You can disable and re-enable logging for a specific resource based on your network administration needs.*

1. On the Main tab, click **Local Traffic** > **Virtual Servers**.
   The Virtual Server List screen opens.
2. Click the name of the virtual server you want to modify.
3. On the menu bar, click **Security** > **Policies**.
   The screen displays firewall rule settings.
4. From the **Log Profile** list, select **Disabled**.
5. Click **Update** to save the changes.

The BIG-IP system does not log the events specified in this profile for the resources to which this profile is assigned.

Implementation result

You now have an implementation in which the BIG-IP® system logs specific Protocol Security events and sends the logs to a specific location.

Appendix
A

IPFIX Templates for AFM DNS Events

Overview: IPFIX Templates for AFM DNS Events

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX Information Elements (IEs) and Templates used to log F5's Application Firewall Manager (AFM) DNS events. An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the denial of a DNS query.

About IPFIX Information Elements for AFM DNS events

Information Elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single Advanced Firewall Manager™ (AFM™) DNS event.

IANA-defined IPFIX Information Elements

IANA maintains a list of standard IPFIX Information Elements (IEs), each with a unique Element Identifier. The F5® AFM™ DNS IPFIX implementation uses a subset of these IEs to publish AFM DNS events. This subset is summarized in the table.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationIPv6Address	28	16
destinationTransportPort	11	2
ingressVRFID	234	4
observationTimeMilliseconds	323	8
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

IPFIX enterprise Information Elements

IPFIX provides for enterprises to define their own Information Elements. F5® currently uses the following non-standard IEs for AFM™ DNS events:

Information Element (IE)	ID	Size (Bytes)
action	12276 - 39	Variable
attackEvent	12276 - 41	Variable
attackId	12276 - 20	4
attackName	12276 - 21	Variable
bigipHostName	12276 - 10	Variable

Information Element (IE)	ID	Size (Bytes)
bigipMgmtIPv4Address	12276 - 5	4
bigipMgmtIPv6Address	12276 - 6	16
contextName	12276 - 9	Variable
deviceProduct	12276 - 12	Variable
deviceVendor	12276 - 11	Variable
deviceVersion	12276 - 13	Variable
dnsQueryType	12276 - 8	Variable
errdefsMsgNo	12276 - 4	4
flowId	12276 - 3	8
ipfixMsgNo	12276 - 16	4
messageSeverity	12276 - 1	1
msgName	12276 - 14	Variable
packetsDropped	12276 - 23	4
packetsReceived	12276 - 22	4
partitionName	12276 - 2	Variable
queryName	12276 - 7	Variable
vlanName	12276 - 15	Variable

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

About individual IPFIX Templates for each event

This section enumerates the IPFIX templates used by F5 to publish AFM DNS Events.

IPFIX template for DNS security

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	

Information Element (IE)	ID	Size (Bytes)	Notes
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
queryName	12276 - 7	Variable	This IE is omitted for NetFlow v9.
dnsQueryType	12276 - 8	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.

IPFIX template for DNS DoS

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
attackEvent	12276 - 41	Variable	This IE is omitted for NetFlow v9.
attackId	12276 - 20	4	
attackName	12276 - 21	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	

Information Element (IE)	ID	Size (Bytes)	Notes
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
queryName	12276 - 7	Variable	This IE is omitted for NetFlow v9.
dnsQueryType	12276 - 8	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
packetsDropped	12276 - 23	4	
packetsReceived	12276 - 22	4	

Appendix
B

IPFIX Templates for AFM SIP Events

Overview: IPFIX Templates for AFM SIP Events

The IP Flow Information Export (IPFIX) Protocol is a logging mechanism for IP events. This appendix defines the IPFIX Information Elements (IEs) and Templates used to log F5's Application Firewall Manager (AFM) events related to the Session Initiation Protocol (SIP). An *IE* is the smallest form of useful information in an IPFIX log message, such as an IP address or a timestamp for the event. An *IPFIX template* is an ordered collection of specific IEs used to record one IP event, such as the acceptance of a SIP session.

About IPFIX Information Elements for AFM SIP events

Information Elements (IEs) are individual fields in an IPFIX template. An IPFIX template describes a single Advanced Firewall Manager™ (AFM™) SIP event.

IANA-defined IPFIX information elements

IANA maintains a list of standard IPFIX Information Elements (IEs), each with a unique Element Identifier. The F5® AFM™ SIP implementation uses a subset of these IEs to publish AFM SIP events. This subset is summarized in the table.

Information Element (IE)	ID	Size (Bytes)
destinationIPv4Address	12	4
destinationIPv6Address	28	16
destinationTransportPort	11	2
ingressVRFID	234	4
observationTimeMilliseconds	323	8
sourceIPv4Address	8	4
sourceIPv6Address	27	16
sourceTransportPort	7	2

IPFIX enterprise Information Elements

IPFIX provides for enterprises to define their own Information Elements. F5® currently uses the following non-standard IEs for AFM™ events:

Information Element (IE)	ID	Size (Bytes)
action	12276 - 39	Variable
attackEvent	12276 - 41	Variable
attackId	12276 - 20	4
attackName	12276 - 21	Variable
bigipHostName	12276 - 10	Variable

Information Element (IE)	ID	Size (Bytes)
bigipMgmtIPv4Address	12276 - 5	4
bigipMgmtIPv6Address	12276 - 6	16
contextName	12276 - 9	Variable
deviceProduct	12276 - 12	Variable
deviceVendor	12276 - 11	Variable
deviceVersion	12276 - 13	Variable
errdefsMsgNo	12276 - 4	4
flowId	12276 - 3	8
ipfixMsgNo	12276 - 16	4
messageSeverity	12276 - 1	1
msgName	12276 - 14	Variable
packetsDropped	12276 - 23	4
packetsReceived	12276 - 22	4
partitionName	12276 - 2	Variable
sipCallee	12276 - 19	Variable
sipCaller	12276 - 18	Variable
sipMethodName	12276 - 17	Variable
vlanName	12276 - 15	Variable

Note: *IPFIX, unlike NetFlow v9, supports variable-length IEs, where the length is encoded within the field in the Data Record. NetFlow v9 collectors (and their variants) cannot correctly process variable-length IEs, so they are omitted from logs sent to those collector types.*

About individual IPFIX Templates for each event

This section enumerates the IPFIX templates used by F5 to publish AFM SIP Events.

IPFIX template for SIP security

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.

Information Element (IE)	ID	Size (Bytes)	Notes
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sipCallee	12276 - 19	Variable	This IE is omitted for NetFlow v9.
sipCaller	12276 - 18	Variable	This IE is omitted for NetFlow v9.
sipMethodName	12276 - 17	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.

IPFIX template for SIP DoS

Information Element (IE)	ID	Size (Bytes)	Notes
action	12276 - 39	Variable	This IE is omitted for NetFlow v9.
attackEvent	12276 - 41	Variable	This IE is omitted for NetFlow v9.
attackId	12276 - 20	4	
attackName	12276 - 21	Variable	This IE is omitted for NetFlow v9.
bigipHostName	12276 - 10	Variable	This IE is omitted for NetFlow v9.
bigipMgmtIPv4Address	12276 - 5	4	
bigipMgmtIPv6Address	12276 - 6	16	
contextName	12276 - 9	Variable	This IE is omitted for NetFlow v9.
observationTimeMilliseconds	323	8	
destinationIPv4Address	12	4	

Information Element (IE)	ID	Size (Bytes)	Notes
destinationIPv6Address	28	16	
destinationTransportPort	11	2	
deviceProduct	12276 - 12	Variable	This IE is omitted for NetFlow v9.
deviceVendor	12276 - 11	Variable	This IE is omitted for NetFlow v9.
deviceVersion	12276 - 13	Variable	This IE is omitted for NetFlow v9.
errdefsMsgNo	12276 - 4	4	
flowId	12276 - 3	8	
ipfixMsgNo	12276 - 16	4	
messageSeverity	12276 - 1	1	
partitionName	12276 - 2	Variable	This IE is omitted for NetFlow v9.
ingressVRFID	234	4	
sipCallee	12276 - 19	Variable	This IE is omitted for NetFlow v9.
sipCaller	12276 - 18	Variable	This IE is omitted for NetFlow v9.
sipMethodName	12276 - 17	Variable	This IE is omitted for NetFlow v9.
sourceIPv4Address	8	4	
sourceIPv6Address	27	16	
sourceTransportPort	7	2	
vlanName	12276 - 15	Variable	This IE is omitted for NetFlow v9.
msgName	12276 - 14	Variable	This IE is omitted for NetFlow v9.
packetsDropped	12276 - 23	4	
packetsReceived	12276 - 22	4	

Index

L

N

P

R

S

T

V

W