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

Version 12.1

Table of Contents

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.

With Advanced Firewall Manager, you can configure the system to automatically track traffic and CPU usage patterns over time, and adapt automatically to possible DoS attacks across a range of DoS vectors. You can configure DoS detection for the whole system, and on an individual, per-DoS-vector basis. Automatic threshold configuration is available for a range of non-error packet types on the AFM system.

With AFM, you can also configure manual responses to DoS vectors. For non-error packets, you can configure absolute packet-per-second limits for attack detection (reporting and logging), percentage increase thresholds for detection, and absolute rate limits on a wide variety of packets that attackers can leverage as attack vectors. In addition, you can configure Bad Actor detection, to identify IP addresses that engage in such attacks, on a per-vector basis, and you can automatically blacklist Bad Actor IP addresses, with specific thresholds and time limits. Configure responses to system-level DoS attack vectors in the DoS Device Configuration.

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 DoS Device Configuration.

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 protocol service attacks

On your BIG-IP® system, you can use different types of profiles to detect and protect against system DoS attacks, to rate limit possible attacks, and to automatically blacklist IP addresses when identified as Bad Actors. You can configure settings for specific protocol attacks for DNS and SIP, and other network attacks.

DoS Protection profile

The DoS Protection profile allows you to configure several settings for DoS protection that you can configure for per-virtual-server DoS detection and prevention. With a DoS protection profile, you can configure several settings.

- Define a source IP address whitelist, to allow addresses to pass through the DoS protection checks.
- Define settings for DNS protocol error detection, which allows you to configure a percentage rate increase over time and a packets-per-second threshold to trigger logging, as well as a hard rate limit on DNS protocol error packets.
- Define packet-per-second rate increases, percentage rate increases, and packet-per-second rate limiting for DNS record types.
- Configure identification, rate limiting, and automatic blacklisting of Bad Actors by DNS query record type. Bad Actors are defined on a packet-per-second level, per record type.
- Define settings for SIP protocol error detection, which allows you to configure a percentage rate increase over time and a packets-per-second threshold to trigger logging, as well as a hard rate limit on SIP protocol error packets.
- Define specific packet-per-second rate increases, percentage rate increases, and packet-per-second rate limiting for SIP request methods.
- Configure identification, rate limiting, and automatic blacklisting of Bad Actors by SIP request method. Bad Actors are defined on a packet-per-second level, per request method.
- Configure identification, rate limiting, and automatic blacklisting of several known network attack types, according to various detection criteria.

DNS Protocol Security profile

The DNS Security profile is a separate profile that you specify in a DNS service profile, to provide security features. The DNS Security Profile allows you to configure the BIG-IP system to exclude (drop) or include (allow) packets of specific DNS query record types. You can also configure the profile to exclude (drop) the DNS QUERY header OpCode.

HTTP Protocol Security profile

The HTTP Security profile allows you to configure the BIG-IP system to perform HTTP protocol checks, HTTP request checks, and to present a blocking page if a check fails. You can attach an HTTP Security profile to a virtual server.

Important: *You can only attach an HTTP security profile to a virtual server that is already configured with an HTTP profile.*

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 Configuration for system-wide DoS protection, and by DoS Profiles for virtual servers. DoS detection features allow you to detect possible attacks on the system and on particular applications, and to rate limit possible attack vectors. AFM also enables further attack mitigation, including automatic identification and blacklisting of attacking IP addresses, and automatic configuration of DoS attack vector thresholds based on system analysis. DoS detection and prevention features are enabled with an Advanced Firewall Manager license, which also includes protocol DoS detection support that can be configured on a per-virtual-server basis.

- At the virtual server level, detect malicious or malformed DNS and SIP protocol errors, and report anomalies by percentage increase, or by absolute packets per second.
- At the virtual server level, rate limit malicious or malformed DNS and SIP protocol error packets.
- At the virtual server level and system-wide, manually configure detection of potential DoS vector attacks by rate increase or absolute packets per second, and rate limit or leak limit such packets.
- System-wide, automatically detect potential attacks across a wide range of DoS attack vectors, and rate limit or leak limit such packets,
- At the virtual server level, detect repeat attackers for SIP, DNS, and other attack vectors and automatically blacklist their IP addresses, with configurable thresholds and blacklist duration.
- System-wide, detect repeat attackers for a wide range of attack vectors and automatically blacklist their IP addresses, with configurable thresholds and blacklist duration.
- At the virtual server level and system-wide, advertise blacklisted IP addresses to BGP routers, per DoS vector and per IP intelligence category. With this option, once an IP address is identified for blacklisting, all further blacklisting of IP addresses is handled by upstream routers, until the blacklist entry is automatically removed.

Task list

Detecting and protecting against system-wide DoS and DDoS attacks
Automatically detecting and protecting against system-wide DoS and DDoS attacks
Configuring manual thresholds for DoS and DDoS vectors

Detecting and protecting against system-wide DoS and DDoS attacks

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

Note: *Not all settings apply to all DoS vectors. For example, some vectors do not use Auto Thresholds, and some vectors cannot be automatically blacklisted.*

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. Configure the Auto Threshold Sensitivity.

   A lower number means the automatic threshold algorithm is less sensitive to changes in traffic and CPU usage.
4. In the **Category** column, expand a category to view and edit the attack types for that category.
5. In the **Attack Type** column, click the name of any attack type to edit the settings.
   - If the attack allows automatic threshold configuration, you can select **Auto-Threshold Configuration** to configure automatic thresholds.
   - To configure manual thresholds, click **Manual Configuration**.
6. Configure the DoS vector for automatic threshold configuration or manual thresholds.
7. Click the **Update** button.
   The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.
8. 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.

Automatically detecting and protecting against system-wide DoS and DDoS attacks

The BIG-IP® system handles DoS and DDoS attacks with preconfigured responses. With the DoS Protection Device Configuration, you can automatically or manually set detection thresholds and internal rate or leak limits for a range of DoS and DDoS attack vectors. Use this task to configure automatic thresholds for the system, and for individual DoS vectors.

Note: *Not all settings apply to all DoS vectors. For example, some vectors do not use Auto Thresholds, and some vectors are not configured for bad actor detection or automatic blacklisting.*

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. Configure the **Auto Threshold Sensitivity**.

   A lower number means the automatic threshold algorithm is less sensitive to changes in traffic and CPU usage.
4. In the **Category** column, expand a category to view and edit the attack types for that category.
5. In the **Attack Type** column, click the name of any attack type to edit the settings.
   The configuration page for the particular attack appears.
6. Select **Auto-Threshold Configuration**.

   Note: *You cannot configure automatic thresholds for every DoS vector. In particular, for error packets you can manually specify only **Detection Threshold PPS**, **Detection Threshold Percent**, and the **Leak Limit**.*

   Note: *You can configure only automatic thresholds or manual thresholds for a DoS vector. When you select one configuration setting, the options for the other setting are grayed out.*

7. In the **Attack Floor PPS** field, specify the number of packets per second of the vector type to allow at a minimum, before automatically calculated thresholds are determined.

   Because automatic thresholds take time to be reliably established, this setting defines the minimum packets allowed before automatic thresholds are calculated.

8. In the **Attack Ceiling PPS** field, specify the absolute maximum allowable for packets of this type, before automatically calculated thresholds are determined.

   Because automatic thresholds take time to be reliably established, this setting rate limits packets to the packets per second setting, when specified. To set no hard limit, set this to **Infinite**.

9. Click the **Update** button.
   The selected configuration is updated, and the DoS Protection Device Configuration screen opens again.
10. 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.

Configuring manual thresholds for DoS and DDoS vectors

You are editing a DoS vector from the **Security** > **DoS Protection** > **Device Configuration** screen.

Manually configure thresholds for a DoS vector when you want to configure specific settings, or when the vector does not allow automatic threshold configuration.

Note: *Not all settings apply to all DoS vectors. For example, some vectors allow* ***Leak Limits*** *instead of* ***Rate Limits****, and some vectors cannot be automatically blacklisted.*

1. If the attack allows automatic or manual threshold configuration, select **Manual Configuration**.
2. 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 registers an attack for the duration that 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.

3. 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 registers an attack for the duration that 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.

4. To log traffic that the system identifies as a DoS attack according to the automatic thresholds, enable **Simulate Auto Threshold.**

   Note: *This setting allows you to see the results of auto thresholds on the selected DoS vector without actually affecting traffic. Automatic thresholds are not applied to packets unless the* ***Auto-Threshold Configuration*** *is enabled for that vector. When you enable this setting, the current computed thresholds for automatic thresholds are displayed for this vector.*

5. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.

6. In the **Per Source IP Detection (PPS)** field, specify the number of packets of this type per second from one IP address that identifies the IP source as a bad actor, for purposes of attack detection and logging.
7. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.
8. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

   Note: *Automatic IP address blacklisting is enabled only when* ***Bad Actor Detection*** *is enabled.*

9. Select the **Blacklist Category** to which blacklist entries generated by **Bad Actor Detection** are added.
10. Specify the **Detection Time**, in seconds, after which an IP address is blacklisted.

    When a Bad Actor IP address exceeds the **Per Source IP Detection PPS** setting for the **Detection Time** period, that IP address is added to the blacklist.
11. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (`14400` seconds).

    After this time period, the IP address is removed from the blacklist.
12. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

    Note: *To advertise to edge routers, you must configure a Blacklist Publisher at* ***Security*** > ***Options*** > ***Blacklist Publisher*** *for the blacklist category.*

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

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, rate-limited, and blacklisted when specified.

Configure SNMP traps, logging, and reporting for DoS attacks, to track threats to your system. Configure a Blacklist Publisher, if necessary, to advertise routes for blacklist entries.

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.

Important: *All hardware-supported vectors are performed in hardware on vCMP® guests, provided that 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
	DNS Malformed	dns-malformed	Malformed DNS packet	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`	Yes

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
			`dos.dnsvlan value`, where `value` is `0-4094`.	
Bad Header - ICMP	Bad ICMP Checksum	bad-icmp-chksum	An ICMP frame checksum is bad. Reuse the TCP or UDP checksum bits in the packet	Yes
	Bad ICMP Frame	bad-icmp-frame	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 • 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	Yes
	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

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
	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-ggt-ip-len	Layer 2 packet length is much greater than the payload length in an IPv4 address header and the layer 2 length is greater than the minimum packet size	Yes
	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-ext-hdr-order	Extension headers in the IPv6 header are in the wrong order	Yes
	Bad IPV6 Hop Count	bad-ipv6-hop-cnt	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

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
	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	ext-hdr-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>	hop-cnt-leq-one	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 Addr	ipv6-bad-src	IPv6 source IP = `0xff00::`	Yes
	IPv6 Extended Header Frames	ipv6-ext-hdr-frames	IPv6 address contains extended header frames	Yes
	IPV6 Length > L2 Length	ipv6-len-gt-l2-len	IPv6 address length is greater than the layer 2 length	Yes
	No L4 (Extended Headers Go To Or Past End of Frame)	l4-ext-hdrs-go-end	Extended headers go to the end or past the end of the L4 frame	Yes
	Payload Length < L2 Length	payload-len-ls-l2-len	Specified IPv6 payload length is less than the L2 packet length	Yes
	Too Many Extended Headers	too-many-ext-hdrs	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
Bad Header - L2	Ethernet MAC Source Address == Destination Address	ether-mac-sa-eq-da	Ethernet MAC source address equals the destination address	Yes
Bad Header - TCP	Bad TCP Checksum	bad-tcp-chksum	The TCP checksum does not match	Yes
	Bad TCP Flags (All Cleared)	bad-tcp-flags-all-clr	Bad TCP flags (all cleared and SEQ#=0)	Yes
	Bad TCP Flags (All Flags Set)	bad-tcp-flags-all-set	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	opt-present-with-illegal-len	Option present with illegal length	Yes

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
	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	tcp-hdr-len-gt-l2-len		Yes
	TCP Header Length Too Short (Length < 5)	tcp-hdr-len-too-short	The Data Offset value in the TCP header is less than five 32-bit words	Yes
	TCP Option Overruns TCP Header	tcp-opt-overruns-tcp-hdr	The TCP option bits overrun the TCP header	Yes
	Unknown TCP Option Type	unk-tcp-opt-type	Unknown TCP option type	Yes
Bad Header - UDP	Bad UDP Checksum	bad-udp-chksum	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
	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	Yes

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
			this value, in tmsh: modify sys db dos.dnsvlan value, where value is 0-4094.	
	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 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 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	Yes

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
			`dos.dnsvlan value`, where `value` is `0-4094`.	
Flood	ARP Flood	arp-flood	ARP packet flood	Yes
	Ethernet Broadcast Packet	ether-brdcst-pkt	Ethernet broadcast packet flood	Yes
	Ethernet Multicast Packet	ether-multicst-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	No
	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
	TCP SYN Oversize	tcp-syn-oversize	Detects TCP data SYN packets larger than the maximum specified by the dos.maxsynsize parameter. To tune this value, in `tmsh`: `modify sys db dos.maxsynsize value`. The default size is `64` and the maximum allowable value is `9216`.	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	Yes

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
	IPv6 Fragment Overlap	ipv6-overlap-frag	IPv6 overlapping fragment error	No
	IPv6 Fragment Too Small	ipv6-short-frag	IPv6 short fragment error	Yes
	IP Fragment Error	ip-other-frag	Other IPv4 fragment error	Yes
	IP Fragment Overlap	ip-overlap-frag	IPv4 overlapping fragment error	No
	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	Yes
	SIP BYE Method	sip-bye-method	SIP BYE packets	Yes
	SIP CANCEL Method	sip-cancel-method	SIP CANCEL packets	Yes
	SIP INVITE Method	sip-invite-method	SIP INVITE packets	Yes
	SIP Malformed	sip-malformed	Malformed SIP packets	Yes
	SIP MESSAGE Method	sip-message-method	SIP MESSAGE packets	Yes
	SIP NOTIFY Method	sip-notify-method	SIP NOTIFY packets	Yes
	SIP OPTIONS Method	sip-options-method	SIP OPTIONS packets	Yes
	SIP OTHER Method	sip-other-method	Other SIP method packets	Yes
	SIP PRACK Method	sip-prack-method	SIP PRACK packets	Yes
	SIP PUBLISH Method	sip-publish-method	SIP PUBLISH packets	Yes
	SIP REGISTER Method	sip-register-method	SIP REGISTER packets	Yes
	SIP SUBSCRIBE Method	sip-subscribe-method	SIP SUBSCRIBE packets	Yes
Bad Header-SCTP	Bad SCTP Checksum	bad-sctp-checksum	Bad SCTP packet checksum	No

DoS category	Attack name	Dos vector name	Information	Hardware accelerated
Other	Host Unreachable	host-unreachable	Host unreachable error	Yes
	IP Unknown protocol	ip-unk-prot	Unknown IP protocol	No
	LAND Attack	land-attack	Source IP equals destination IP address	Yes
	TIDCMP	tidcmp	ICMP source quench attack	Yes

Preventing DoS Sweep and Flood Attacks

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 exceed the rate limit, are dropped. You can also configure the Sweep vector to automatically blacklist an IP address from which the Sweep attack originates.

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 verify 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 exceed 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 DoS Protection: Device Configuration.

Task list

Detecting and protecting against single endpoint DoS flood attacks
Detecting and protecting against DoS sweep attacks
Detecting and protecting against UDP flood attacks
Allowing individual addresses to bypass DoS checks

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 registers an attack for the duration that 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 **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 no longer exceeds.
   - 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, and automatically blacklist IP addresses that you detect perpetrating such 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 registers an attack for the duration that 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 **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 no longer exceeds.
- 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. In the Additional Actions area, select **Categorize address** and configure the settings. You can select a black list category from the list, specify the detection time in seconds after which the attacking endpoint is blacklisted, and specify the duration for which the address remains assigned to the category. By default, the configuration adds an IP address to the blacklist after one minute (60 seconds), and the IP address is blacklisted for 4 hours (14400 seconds).
9. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (`14400` seconds).
10. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

    Note: *To advertise to edge routers, you must configure a Blacklist Publisher at **Security** > **Options** > **Blacklist Publisher** for the blacklist category.*

11. 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, to allow such attacks to be identified in system logs and reports, and to automatically add such attackers to a blacklist of your choice.

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 registers an attack for the duration that 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 registers an attack for the duration that 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 **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 no longer exceeds.
   - 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 individual addresses to bypass DoS checks

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. To use an address list as a source whitelist, select the address list from **Source Address List**.
3. Click **Create**.
   The New White List Configuration screen opens.
4. In the **Name** field, type a name for the whitelist entry.
5. In the **Description** field, type a description for the whitelist entry.
6. From the **Protocol** list, select the protocol for the whitelist entry.

   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.

7. 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.
8. 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.
9. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and start 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.

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 rate limit DNS packets that have errors that could be considered malicious.
- To log unusual increases in DNS packets that contain errors, or DNS Query packets that rapidly increase, and to rate limit such packets.

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 rate limit DNS query packets.

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 list

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

Creating a custom DNS profile to firewall DNS traffic

Assigning a DNS profile to a virtual server

Associating a DoS profile with a virtual server

Allowing individual addresses to bypass DoS checks

Creating a custom DoS Protection Logging profile to log DNS attacks

Configuring an LTM virtual server for DoS Protection event logging

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 detecting percentage increase in packets 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. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
4. To configure DNS security settings, click **Protocol DNS**, click **Edit** in the far right column, then select **Enabled**.

5. To enable attack detection based on the rate of protocol errors, next to **Protocol Errors Attack Detection**, click **Edit** in the far right column, then 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. In the **Rate threshold** field, type the rate of packets with errors per second to detect.

   This threshold sets an absolute limit which, when exceeded, registers an attack.
8. In the **Rate limit** field, type the absolute limit for packets per second with protocol errors. Packets that exceed this limit are dropped.
9. To change the threshold or rate increase for a particular DNS record, in the DNS Query Attack Detection area, click **Edit** in the far right column, select the **Enabled** check box for each record type that you want to configure, then change the values for **Threshold**, **Rate Increase**, and **Rate Limit** in the associated fields.

   For example, to change the detection threshold for IPv6 address requests to 9,999 per second, or an increase of 250% over the average, select the **Enabled** check box next to **aaaa**, then set the **Threshold** field to `9999` and the **Rate Increase** field to `250`. To rate limit such requests to 33,000 packets per second, set the **Rate Limit** field to `33000`.

   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. However, packets are dropped at the* ***Rate Limit*** *setting, not at the attack detection threshold.*

10. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.
11. In the **Per Source IP Detection (PPS)** field, specify the number of packets of this type per second from one IP address that identifies the IP source as a bad actor, for purposes of attack detection and logging.
12. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.
13. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

    Note: *Automatic IP address blacklisting is enabled only when* ***Bad Actor Detection*** *is enabled.*

14. Specify the **Detection Time**, in seconds, after which an IP address is blacklisted.

    When a Bad Actor IP address exceeds the **Per Source IP Detection PPS** setting for the **Detection Time** period, that IP address is added to the blacklist.
15. To change the duration for which the address is blacklisted, specify the duration in seconds in the **Duration** field. The default duration for an automatically blacklisted item is 4 hours (`14400` seconds).

    After this time period, the IP address is removed from the blacklist.
16. Select the **Blacklist Category** to which blacklist entries generated by **Bad Actor Detection** are added.
17. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

    Note: *To advertise to edge routers, you must configure a Blacklist Publisher at* ***Security*** > ***Options*** > ***Blacklist Publisher*** *for the blacklist category.*

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

You have now configured a DoS Protection profile to provide custom responses to malicious DNS attacks, and DNS flood attacks, to allow such attacks to be identified in system logs and reports, and to allow rate limiting of such attacks. DNS queries on particular record types you have configured in the DNS Query Attack Detection area are detected as attacks at your specified thresholds and rate increases, and rate limited as specified.

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.

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. On the menu bar, 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 individual addresses to bypass DoS checks

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. To use an address list as a source whitelist, select the address list from **Source Address List**.
3. Click **Create**.
   The New White List Configuration screen opens.
4. In the **Name** field, type a name for the whitelist entry.
5. In the **Description** field, type a description for the whitelist entry.
6. From the **Protocol** list, select the protocol for the whitelist entry.

   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
7. 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.
8. 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.
9. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and start 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 to log DNS attacks

Create a custom Logging profile to log DNS DoS 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 **Protocol Security** check box, to enable the BIG-IP® system to log HTTP, FTP, DNS, and SMTP protocol request events.
4. From the **Log Publisher** list, select a destination to which the BIG-IP system sends DNS log entries.
5. Select the **Log Dropped Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
6. Select the **Log Filtered Dropped 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.*

7. Select the **Log Malformed Requests** check box, to enable the BIG-IP system to log malformed DNS requests.
8. Select the **Log Rejected Requests** check box, to enable the BIG-IP system to log rejected DNS requests.
9. Select the **Log Malicious Requests** check box, to enable the BIG-IP system to log malicious DNS requests.
10. 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.

11. Select the **DoS Protection** check box.
12. 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.
13. 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 network firewall security 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.

Detecting and preventing 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.

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

Task list

Detecting SIP denial-of-service attacks with a DoS profile
Assigning a SIP profile to a virtual server
Associating a DoS profile with a virtual server
Allowing individual addresses to bypass DoS checks
Creating a custom SIP DoS Protection Logging profile
Configuring an LTM virtual server for DoS Protection event logging

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. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
4. To configure SIP security settings, click **Protocol SIP Protection**, click **Edit** in the far right column, then select **Enabled**.
5. To enable attack detection based on the rate of protocol errors, next to **Protocol Errors Attack Detection**, click **Edit** in the far right column, then 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. In the **Rate threshold** field, type the rate of packets with errors per second to detect.

   This threshold sets an absolute limit which, when exceeded, registers an attack.
8. In the **Rate limit** field, type the absolute limit for packets per second with protocol errors. Packets that exceed this limit are dropped.
9. To change the threshold or rate increase for a particular SIP method, in the **SIP Method Attack Detection** settings, click **Edit** in the far right column, select the **Enabled** check box for each request 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 threshold for NOTIFY requests to 9,999 per second, or an increase of 250% over the average, select the **Enabled** check box next to **notify**, then set the Threshold field to `9999` and the Rate Increase field to `250`. To rate limit such requests to 33,000 packets per second, set the **Rate Limit** field to `33000`.

   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, packets are dropped at the* ***Rate Limit*** *setting, not at the attack detection threshold.*
10. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.
11. In the **Per Source IP Detection (PPS)** field, specify the number of packets of this type per second from one IP address that identifies the IP source as a bad actor, for purposes of attack detection and logging.
12. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.
13. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

    Note: *Automatic IP address blacklisting is enabled only when* ***Bad Actor Detection*** *is enabled.*
14. In the **Blacklist Detection Period** field, specify the duration in seconds after which the attacking endpoint is blacklisted. By default, the configuration adds an IP address to the blacklist after one minute (60 seconds). **Enabled**.
15. In the **Blacklist Duration** field, specify the amount of time in seconds that the address will remain on the blacklist. The default is `14400` (4 hours).
16. From the **Blacklist Category** list, select a black list category to apply to automatically blacklisted addresses.
17. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

    Note: *To advertise to edge routers, you must configure a Blacklist Publisher at* ***Security*** > ***Options*** > ***Blacklist Publisher*** *for the blacklist category.*
18. 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. On the menu bar, 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 individual addresses to bypass DoS checks

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. To use an address list as a source whitelist, select the address list from **Source Address List**.
3. Click **Create**.

The New White List Configuration screen opens.

4. In the **Name** field, type a name for the whitelist entry.
5. In the **Description** field, type a description for the whitelist entry.
6. From the **Protocol** list, select the protocol for the whitelist entry.

   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
7. 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.
8. 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.
9. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and start 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 network firewall security 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.

Detecting and Preventing Network DoS Attacks

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

Network DoS protection is a type of security that collects several DoS checks in a DoS security profile. Attack detection and prevention serves two functions:

- To detect and report on packets based on behavior characteristics of the sender or characteristics of the packets.
- To detect, report, and rate limit unusual increases in packets that signify specific known attack vectors.

You can configure the Network DoS Protection profile to detect possible attack vectors by packet-per-second or percentage-increase-over-time thresholds, which can indicate that a possible attack is in process. Such attacks can be logged and reported through system logging facilities. You can also rate limit packets of known vectors.

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.

DoS protection requires that your virtual server includes a DoS profile that includes network security.

Task list

Detecting and protecting against network denial-of-service attacks with a DoS profile
Associating a DoS profile with a virtual server
Allowing individual addresses to bypass DoS checks
Allowing a list of addresses to bypass DoS checks
Creating a custom Network Firewall Logging profile
Configuring an LTM virtual server for DoS Protection event logging

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

You can configure network attack settings in a DoS profile.

The BIG-IP® system handles network attacks that use malformed packets and malicious attack vectors. Possible malicious packets and attacks are detected by logging when packets exceed a threshold of packets per second, and by detecting the rate increase percentage in packets of a certain type over time. You can configure settings to identify and rate limit possible network attacks with a DoS profile. For sweep packets, you can also automatically blacklist IPs.

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. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
4. To configure network security settings, under **Network** click General Settings, click **Edit** in the far right column, then select **Enabled**.

5. To change the threshold or rate increase for a particular network attack, in the Network Attack Types area, click **Edit** in the far right column, select the **Enabled** check box for each attack type that you want to configure, then change the values for **Threshold**, **Rate Increase**, and **Rate Limit** in the associated fields.

   For example, to change the detection threshold for IP fragments to 9,999 per second, or an increase of 250% over the average, in Attack Types, click IP Fragment Flood, click the **Enabled** check box next to **IP Fragment Flood**, then set the **Threshold** field to `9999` and the **Rate Increase** field to `250`. To rate limit such requests to 33,000 packets per second, set the **Rate Limit** field to `33000`.

   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: *The Attack Types area allows you to configure the thresholds at which the firewall registers an attack. However, packets are dropped at the* ***Rate Limit*** *setting, not at the attack detection threshold.*

6. To detect IP address sources from which possible attacks originate, enable **Bad Actor Detection**.
7. In the **Per Source IP Detection (PPS)** field, specify the number of packets of this type per second from one IP address that identifies the IP source as a bad actor, for purposes of attack detection and logging.
8. In the **Per Source IP Rate Limit (PPS)** field, specify the number of packets of this type per second from one IP address, above which rate limiting or leak limiting occurs.
9. To automatically blacklist bad actor IP addresses, select **Blacklist Attacking Address**.

   Note: *Automatic IP address blacklisting is enabled only when* ***Bad Actor Detection*** *is enabled.*

10. In the **Blacklist Detection Period** field, specify the duration in seconds after which the attacking endpoint is blacklisted. By default, the configuration adds an IP address to the blacklist after one minute (60 seconds). **Enabled**.
11. In the **Blacklist Duration** field, specify the amount of time in seconds that the address will remain on the blacklist. The default is `14400` (4 hours).
12. From the **Blacklist Category** list, select a black list category to apply to automatically blacklisted addresses.
13. To allow IP source blacklist entries to be advertised to edge routers so they will null route their traffic, select **Allow Advertisements**.

    Note: *To advertise to edge routers, you must configure a Blacklist Publisher at* ***Security*** > ***Options*** > ***Blacklist Publisher*** *for the blacklist category.*

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

You have now configured a DoS Protection profile to analyze network packet behavior for DoS attacks, to allow specific configured attacks to be identified in system logs and reports, and to allow rate limiting of such attacks. DNS queries on particular record types you have configured in the DNS Query Attack Detection area are detected as attacks at your specified thresholds and rate increases, and rate limited as specified.

Associate the DoS profile with a virtual server to enable network DoS protection.

Detecting and protecting against DoS sweep attacks with a DoS profile

Within a DoS profile, you can set detection thresholds and rate limits for DoS sweep attacks, and automatically blacklist IP addresses that you detect perpetrating such attacks. Use the DoS profile where you want greater granularity than the Device DoS settings, because you can attach the DoS profile to a virtual server.

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. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
4. To configure network security settings, under **Network** click General Settings, click **Edit** in the far right column, then select **Enabled**.
5. To change the threshold, rate increase, rate limit, and blacklist settings for a sweep attack, in the Network Attack Types area, click **Edit** in the far right column, select **Sweep**, and select the **Enabled** check box. Change the values for **Threshold**, **Rate Increase**, and **Rate Limit** in the associated fields.

   For example, to change the detection threshold for IP fragments to 9,999 per second, or an increase of 250% over the average, in Attack Types, click IP Fragment Flood, click the **Enabled** check box next to **IP Fragment Flood**, then set the **Threshold** field to `9999` and the **Rate Increase** field to `250`. To rate limit such requests to 33,000 packets per second, set the **Rate Limit** field to `33000`.

   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: *The Attack Types area allows you to configure the thresholds at which the firewall registers an attack. However, packets are dropped at the* ***Rate Limit*** *setting, not at the attack detection threshold.*

6. Next to **Auto-blacklisting**, select **Enabled**.
7. In the **Blacklist Detection Period** field, specify the duration in seconds after which the attacking endpoint is blacklisted. By default, the configuration adds an IP address to the blacklist after one minute (60 seconds). **Enabled**.
8. In the **Blacklist Duration** field, specify the amount of time in seconds that the address will remain on the blacklist. The default is `14400` (4 hours).
9. From the **Blacklist Category** list, select a black list category to apply to automatically blacklisted addresses.
10. Click **Update** to save your changes.

You have now configured a DoS Protection profile to automatically blacklist IP addresses that employ sweep attacks. Sweep attacks are also logged and rate-limited at the specified thresholds and limits.

Associate the DoS profile with a virtual server to enable network DoS protection.

DoS profile attack types

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

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

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
+	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

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
+	IP Option Frames	ip-opt-frames	IPv4 address packet with `option.db variable tm.acceptipsourceroute` must be enabled to receive IP options	Yes
+	IPv6 extension header too large	ext-hdr-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>	hop-cnt-leq-one	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
+	IPv6 Extended Header Frames	ipv6-ext-hdr-frames	IPv6 address contains extended header frames	Yes
+	Too Many Extended Headers	too-many-ext-hdrs	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
+	Option Present With Illegal Length	opt-present-with-illegal-len	Option present with illegal length	Yes
+	TCP Bad URG	tcp-bad-urg	Packet contains a bad URG flag, this is likely malicious	Yes
+	TCP Option Overruns TCP Header	tcp-opt-overruns-tcp-hdr	The TCP option bits overrun the TCP header.	Yes
+	Unknown TCP Option Type	unk-tcp-opt-type	Unknown TCP option type	Yes
+	ICMPv4 Flood	icmpv4-flood	Flood with ICMP v4 packets	Yes
+	ICMPv6 Flood	icmpv6-flood	Flood with ICMP v6 packets	Yes
+	IP Fragment Flood	ip-frag-flood	Fragmented packet flood with IPv4	Yes
+	IPv6 Fragment Flood	ipv6-frag-flood	Fragmented packet flood with IPv6	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 exceeds the maximum. To tune this value, in tmsh: `modify sys db dos.tcplowwindowsize value`, where `value` is <=`128`.	Yes
+	TCP SYN Oversize	tcp-syn-oversize	Detects TCP data SYN packets larger than the maximum specified by the dos.maxsynsize	Yes

DoS Category	Attack Name	Dos Vector Name	Information	Hardware accelerated
			parameter. To tune this value, in tmsh: `modify sys db dos.maxsynsize value`. The default size is `64` and the maximum allowable value is `9216`.	
+	UDP Flood	udp-flood	UDP flood attack	Yes
+	ICMP Fragment	icmp-frag	ICMP fragment flood	Yes
+	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. You can also configure automatic blacklisting for IPs that initiate sweep attacks, using the IP intelligence mechanism.	No
+	Host Unreachable	host-unreachable	Host unreachable error	Yes
+	TIDCMP	tidcmp	ICMP source quench attack	Yes

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. On the menu bar, 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 individual addresses to bypass DoS checks

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. To use an address list as a source whitelist, select the address list from **Source Address List**.

3. Click **Create**.
   The New White List Configuration screen opens.
4. In the **Name** field, type a name for the whitelist entry.
5. In the **Description** field, type a description for the whitelist entry.
6. From the **Protocol** list, select the protocol for the whitelist entry.

   The options are **Any**, **TCP**, **UDP**, **ICMP**, or **IGMP**.
7. 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.
8. 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.
9. Click **Finished** to add the whitelist entry to the configuration. Click **Repeat** to add the whitelist entry, and start 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.

Allowing a list of addresses to bypass DoS checks

You can select a specific list of whitelist addresses that the DoS profile does not subject to DoS checks.

1. On the Main tab, click **Security** > **DoS Protection** > **DoS Profiles**.
   The DoS Profiles list screen opens.
2. Click the name of an existing DoS profile (or create a new one).
   The DoS Profile Properties screen for that profile opens.
3. From the list of **Source IP Address Whitelist** items, select the address list to apply as whitelisted addresses to the DoS profile.
4. Click **Update** to add the whitelist to the configuration.

You have now added a list of whitelist addresses that are allowed to bypass DoS checks to the DoS profile.

Creating a custom Network Firewall Logging profile

Create a custom Logging profile to log messages about BIG-IP® system Network Firewall events.

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. In the **Name** field, type a unique name for the profile.
4. Select the **Network Firewall** check box.
5. In the Network Firewall area, from the **Publisher** list, select the publisher the BIG-IP system uses to log Network Firewall events.
6. Set an **Aggregate Rate Limit** to define a rate limit for all combined network firewall log messages per second. Beyond this rate limit, log messages are not logged.

7. For the **Log Rule Matches** setting, select how the BIG-IP system logs packets that match ACL rules. You can select any or all of the options. When an option is selected, you can configure a rate limit for log messages of that type.

Option	Description
Option	Enables or disables logging of packets that match ACL rules configured with:
Accept	`action=Accept`
Drop	`action=Drop`
Reject	`action=Reject`

8. Select the **Log IP Errors** check box, to enable logging of IP error packets. When enabled, you can configure a rate limit for log messages of this type.
9. Select the **Log TCP Errors** check box, to enable logging of TCP error packets. When enabled, you can configure a rate limit for log messages of this type.
10. Select the **Log TCP Events** check box, to enable logging of open and close of TCP sessions. When enabled, you can configure a rate limit for log messages of this type.
11. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for Network Firewall log events.
12. Enable the **Log Geolocation IP Address** setting to specify that when a geolocation event causes a network firewall action, the associated IP address is logged.
13. 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.

14. In the IP Intelligence area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log source IP addresses, which are identified and configured for logging by an IP Intelligence policy.

    Note: *The IP Address Intelligence feature must be enabled and licensed.*

15. Set an **Aggregate Rate Limit** to define a rate limit for all combined IP Intelligence log messages per second. Beyond this rate limit, log messages are not logged.
16. Enable the **Log Translation Fields** setting to log both the original IP address and the NAT-translated IP address for IP Intelligence log events.

17. In the Traffic Statistics area, from the **Publisher** list, select the publisher that the BIG-IP system uses to log traffic statistics.
18. Enable the **Active Flows** setting to log the number of active flows each second.
19. Enable the **Reaped Flows** to log the number of reaped flows, or connections that are not established because of system resource usage levels.
20. Enable the **Missed Flows** setting to log the number of packets that were dropped because of a flow table miss. A flow table miss occurs when a TCP non-SYN packet does not match an existing flow.
21. Enable the **SYN Cookie (Per Session Challenge)** setting to log the number of SYN cookie challenges generated each second.
22. Enable the **SYN Cookie (White-listed Clients)** setting to log the number of SYN cookie clients whitelisted each second.
23. Click **Finished**.

Assign this custom network firewall 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 network firewall security 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.

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.

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.*

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

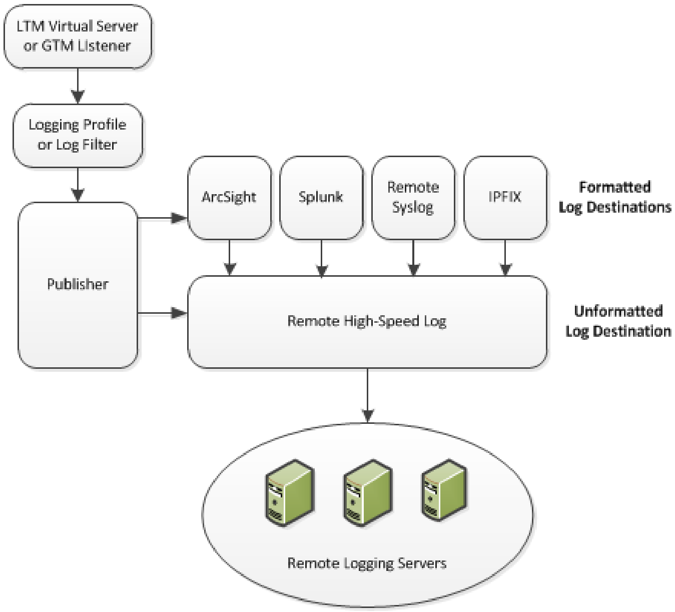

LTM Virtual Server or GTM Listener
Logging Profile or Log Filter
Publisher
ArcSight
Splunk
Remote Syslog
IPFIX
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destination
Remote Logging Servers

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

About the configuration objects of DoS Protection event logging

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	Applies to
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP® system can send log messages.	Creating a pool of remote logging servers.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.	Creating a remote high-speed log destination.
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.	Creating a formatted remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.	Creating a publisher.
DNS Logging profile	Create a custom DNS Logging profile to define the data you want the BIG-IP system to include in the DNS logs and associate a log publisher with the profile.	Creating a custom DoS Protecttion Logging profile.
LTM® virtual server	Associate a custom DNS profile with a virtual server to define how the BIG-IP system logs the DNS traffic that the virtual server processes.	Configuring an LTM virtual server for DoS Protection event 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 network firewall security 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 network firewall security 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.

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.

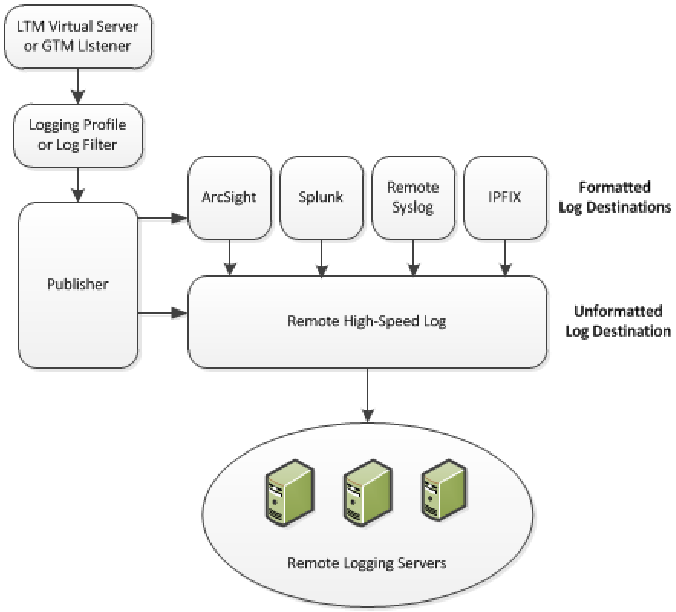

LTM Virtual Server or GTM Listener
Logging Profile or Log Filter
Publisher
ArcSight
Splunk
Remote Syslog
IPFIX
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destination
Remote Logging Servers

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.

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 network firewall security 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 network firewall security 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.

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 list

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.

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.

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.

Task list

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. Under Profile Information, click **General Settings**, and 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. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
6. Under Profile Information, click **General Settings**, and in the **Profile Name** field, type the name for the profile.
7. Under Profile Information, click **General Settings**, and 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.

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.

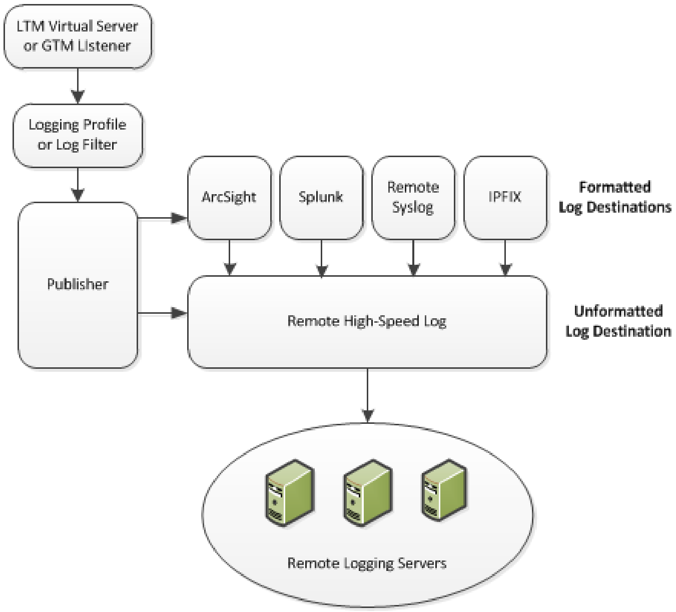

LTM Virtual Server or GTM Listener
Logging Profile or Log Filter
Publisher
ArcSight
Splunk
Remote Syslog
IPFIX
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destination
Remote Logging Servers

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 network firewall security 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 network firewall security 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.

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.

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.

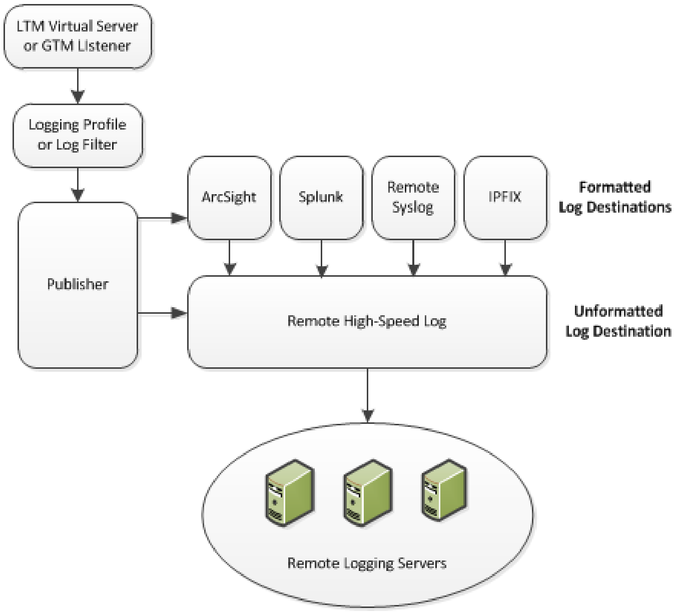
Configuring High-Speed Remote Logging of Protocol Security Events

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.*

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



LTM Virtual Server or GTM Listener
Logging Profile or Log Filter
Publisher
ArcSight
Splunk
Remote Syslog
IPFIX
Formatted Log Destinations
Remote High-Speed Log
Unformatted Log Destination
Remote Logging Servers

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

About the configuration objects of remote 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	Applies to
Pool of remote log servers	Create a pool of remote log servers to which the BIG-IP® system can send log messages.	Creating a pool of remote logging servers.
Destination (unformatted)	Create a log destination of Remote High-Speed Log type that specifies a pool of remote log servers.	Creating a remote high-speed log destination.
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.	Creating a formatted remote high-speed log destination.
Publisher	Create a log publisher to send logs to a set of specified log destinations.	Creating a publisher.
DNS Logging profile	Create a custom DNS Logging profile to define the data you want the BIG-IP system to include in the DNS logs and associate a log publisher with the profile.	Creating a custom Protocol Security Logging profile.
LTM® virtual server	Associate a custom DNS profile with a virtual server to define how the BIG-IP system logs the DNS traffic that the virtual server processes.	Configuring a virtual server for Protocol Security event 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 Requests** check box, to enable the BIG-IP system to log dropped DNS requests.
7. Select the **Log Filtered Dropped 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 Requests** check box, to enable the BIG-IP system to log malformed DNS requests.
9. Select the **Log Rejected Requests** check box, to enable the BIG-IP system to log rejected DNS requests.
10. Select the **Log Malicious 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 network firewall security 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 network firewall security 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.

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

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

Information Element (IE)	ID	Size (Bytes)	Notes
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	
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.

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.
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	

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

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

Information Element (IE)	ID	Size (Bytes)	Notes
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	
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	

Information Element (IE)	ID	Size (Bytes)	Notes
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	
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	

Legal Notices

Legal notices

Publication Date

This document was published on May 9, 2016.

Publication Number

MAN-0440-05

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

Trademarks

For a current list of F5 trademarks and service marks, see *http://www.f5.com/about/guidelines-policies/trademarks/*.

All other product and company names herein may be trademarks of their respective owners.

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.

Index