Oracle® SD-WAN Edge 7.3

Configuration File Reference

Original Publication Date: Nov 1, 2019

Table of Contents

About This Document

This document provides a comprehensive listing of the options and settings available for configuration of an Oracle SD-WAN running Talari Adaptive Private Networking (APN) 6.1. The reader of this document is expected to be a network administrator.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
    - For technical issues such as creating a new Service Request (SR), select 1.
    - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability

- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click Industries.
3. Click the Oracle Communications link.

   Under the SD-WAN header, select a product.
4. Select the Release Number.

   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the PDF link, select Save target as (or similar command based on your browser), and save to a local folder.

References

The following documents are available:

- *Talari Glossary*
- *Talari WAN Implementation Guide*
- *Talari Appliance Quick Start Guide*
- *Talari APN 6.1 New Features Guide*
- *Talari APN 6.1 GA Release Notes*

Configuration File

Oracle Talari Appliances are configured via a single Talari Configuration File that is loaded, validated, and applied by the Talari Appliance functioning as the Network Control Node (NCN). Unlike typical Command Line Interface (CLI) configuration schemes, a Talari WAN (also known as an Adaptive Private Network (APN)) is configured offline. The Talari Configuration File is processed by the APN Configuration Compiler, which provides instant feedback and verification so that errors may be corrected before the configuration is applied to the production network.

In the following sections, the structure, language, and defaults of the Talari Configuration File are described in detail. For instructions on compiling a Talari Configuration File and applying it to an APN, see the *Talari Appliance Quick Start Guide* and the *Talari APN Configuration Editor Demo Video*.

Structure

The Talari Configuration File is a text file consisting of a set of object definition blocks, each of which includes a set of commands, which in turn include sets of parameters. Comments, as described below, may be inserted anywhere in the configuration file.

Comments

Comments are sections of a configuration file that are not to be compiled. When working on a configuration, it is helpful for the administrator to add comments to the file for later reference or to disable a section of the configuration without deleting it. The Talari Configuration File supports two types of comments: single line and multiple line. Single line comments begin with a double slash and cause all text between the double slash and the end of the line to be ignored by the compiler. Multiple line comments begin with a single slash immediately followed by an asterisk and end with an asterisk immediately followed by a slash. All text in between is ignored by the compiler. The user may comment within a configuration file using one of two methods, which are the same as C/C++ comment convention.

- Place a “//” in line — all following text until end of line will be ignored by the compiler.
- Place a “/*” followed by text ending in “*/” — all enclosed text will be ignored by the compiler.
- Nested comments are supported.

Syntax

The Talari Configuration File is organized in to network object definition blocks. Within each object definition, a specific set of commands is available, each of which allows the setting of certain parameters. The general format for an object definition is:

```
define object [name=text]
{
    command1
    command2
    ...
    commandN
}
```

Commands come in three variations. The “set” command is used when configuring a variable that exists with a default value even when “set” is not explicitly issued:

```
set command
    param1=value
    param2=value
    ...
    paramN=value;
```

The “add” command is used when creating a configured instance of an entity that would not exist if not defined:

```
add command
    param1=value
    param2=value
    ...
    paramN=value;
```

When an “add” command allows subcommands, brackets are used:

```
add command
{
    command1
    command2
    ...
    commandN
}
```

The configuration compiler is not sensitive to white space, so indentation, tabs, spaces, and new lines may be used according to the preference of the administrator. The compiler is also sequence insensitive, with the exception of the “add rule” command, which is explained in the next section. All other commands, as well as object definitions and parameter lists may be ordered according to the preference of the administrator.

Each parameter must be assigned a value consistent with the parameter type. Certain parameters require sub parameters, in which case the value of each parameter is a bracket enclosed “{...}” set of sub-parameters and their values.

Parameter Types and Naming Conventions

The following table provides details on the different parameter types and naming conventions:

Type	Format	Constraints	Suffix	Example
Text	cccc	<=32 characters, each of which is an alphanumeric, dash, or underscore; first character must be a letter, not a number.	None	London NewYork Home_Office Data-Center
IP Address	X.X.X.X	0<=X<=255	_addr	192.168.51.175
Network Address	X.X.X.X/n	0<=X<=255; 0<=n<=32; if no subnet prefix given, /32 is assumed	_addrn	192.168.51.1/24
Number	N	integer, N>=0	_kbps, _bytes, _ms	512
Class ID	N	integer, 0 <= N <= 16	_id	5
Percent	N	integer, 0 <= n <= 100	_pct	75
Decimal Percent	N.N	float, 0.0 <= n <= 100.0	_pct	10.1
Hex Number	0xH	A hexadecimal number prefixed with “0x”	None	0x1a2e
Boolean	YES/NO, or TRUE/FALSE		None	yes
Email Address	text@text.text	Valid email address	None	bob@abc.com
Range	X-Y	X < Y	None	12-25
MAC Address	YY:YY:YY:XX:XX:XX	Base Mac address to be used for all Virtual Mac	None	EA:CA:FE:00:00:00

Type	Format	Constraints	Suffix	Example
		addresses – YY:YY:YY. Additional internal values are used to complete the mac address – XX:XX:XX.		

Configuration File Parameters

This section describes the configuration language in detail. Each network object definition subsection includes a description of syntax along with a list of available commands and their associated parameters.

APN Properties

Syntax

Note: All parameters listed in square brackets [] are optional.

```
[set apn_properties]
        [encryption_mode={aes128|aes256}]
        [encryption_rekey_enabled={yes|no}]
        [enhanced_message_authentication={yes|no}]
        [enhanced_message_authentication_type={checksum|sha256}]
        [enhanced_packet_uniqueness={yes|no}] ;
```

set advanced_properties

Keyword	Type	Description	Required	Default
activate_standby_bandwidth_threshold_percentage	number	This is the percentage of the total fair share rates of the associated WAN links in a conduit. When the available bandwidth provided by the regular active WAN links in a conduit drops below this threshold, on-demand standby WAN links are activated to supplement bandwidth.	Yes, but only when on-demand standby wan links are configured	N/A

Site

This object defines an enterprise site for the APN configuration. The site name is referenced in other parts of the configuration file.

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define site name=text
{
        add appliance name=text
        {
                set appliance_properties
                        secure_key=key
        model={vt800|t510|t730|t750|t3000|t3010|t5000|t5200|t860|ct800|e100|e1000|e50}
```

```
                [license=text]
                [license_rate=n]
                [appliance_mode={client | primary_ncn | secondary_ncn}]
                        [enable_wan_to_wan_forwarding={yes | no}]
                        [enable_src_mac_learning={yes|no}]
                        [wan_to_wan_forwarding_route_cost=n]
                        [default_direct_route_cost=n]
                        [is_intermediate_site ={yes|no}]
                        [wan_to_wan_forwarding_group=text]
                        [persist_ucast_refresh_time_ms=n]
                        [max_dynamic_conduits_for_site=n]
              [enable_conduit_to_conduit_forwarding={yes | no}]
              [enable_conduit_to_ii_forwarding={yes | no}]
                        [application_normal_rtt_adjust_ms=n]
                        [application_warning_rtt_adjust_ms=n]

        ;

                add site_routing_domain name=text
        {
                set site_routing_domain_properties
                        is_default={yes|no}
                ;
        }

                add interface_group
                {
                        [set properties]
                                [secure_zone={trusted | untrusted}]
                                [bypass_mode={fail_to_block | fail_to_wire}]
                    [is_bridged={yes|no}]

                        add ethernet_interface
                                device={1 | 2 }; //vt100 or vt500
                                device={1 | 2 | 3}; //t200 or t510

                                device={1 | 2 | 3 | 4 | 5 | 6 | X1}; //t700
                                device={1 | 2 | 3 | 4 | 5 | X1 | X2 | X3 | X4}; //t730 or t750
or t860
                                device={1 | 2 | 3 | 4 | 5} //t3000 or t3010
                                device={1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | AUX} //t5000 or t5200
                             device={1 | 2| 3 | 4 }; //ct800
                                device={1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | AUX}
//e1000
                                device={1 | 2 | 3 | 4 | 5 } //e100
                               device={1 | 2 | 3 } //e50
                        Note: The 4.1 specifies only device 3 Ethernet Interface ports
including the management port, but the software will allow for configuring 1 | 2| 3 | 4 for
flexible support. Testing and support in R4.1 will be limited to ethernet_interface device
                1                       |                       2
```

```
                add virtual_interface
                        name=text
                        [vlan_id={native | 0...4094}];
                        [routing_domain=text]
                        [is_dhcp_client=[true|false]]
        [firewall_zone=text];


                [add bridge_pair]
                        device_one = {1|2|3|4|5|6|7|8|X1|X2|X3|X4}
                [device_two      =      {1|2|3|4|5|6|7|8|X1|X2|X3|X4};
                is_port_state_reflection_enabled={yes|no};
        }

        add virtual_ip_addrn
                virtual_interface_name=text
                ip_addrn=x.x.x.x/n;
        is_identity=[yes | no]
        is_private=[yes|no]
;

add dynamic_conduit_service
{
}
[add dhcp]
{
        [add dhcp_subnet]
        {
                set dhcp_subnet_properties
                        virtual_interface_name=text
                        [domain_name=text]
                        [primary_dns=x.x.x.x]
                        [secondary_dns=x.x.x.x]
                        [enabled={yes|no}]
                ;
                add dhcp_subnet_range
                        range_start=x.x.x.x
                        range_end=x.x.x.x
                        [gateway=x.x.x.x]
                        [option_set_name=text]
                ;
                [add dhcp_subnet_host]
                        fixed_ip_addr=x.x.x.x
                        mac_addr= xx:xx:xx:xx:xx:xx
                        [option_set_name=text]
                ;
        }

        [add dhcp relay]
```

```
                        virtual_interface_name=text
                        server_ip=x.x.x.x
                        server_ip2=x.x.x.x
                        server_ip3=x.x.x.x
                        server_ip4=x.x.x.x
                ;         }
        add dns_proxy
        {
                set dns_proxy_properties
                        routing_domain=text
                        [primary_dns_server_ip=ip]
                        [primary_use_dhcp_client_dns=yes|no]
                        [secondary_dns_server_ip=ip]
                        [secondary_use_dhcp_client_dns=yes|no]
                ;
                add override_dns_server
                        match_domain=text
                        primary_dns_server_ip=ip
                        [secondary_dns_server_ip=ip]
                ;
        }
        add lan_gre_tunnel
                tunnel_name=text
                src_ip=x.x.x.x
            dest_ip=x.x.x.x
                tunnel_ip_addrn=x.x.x.x/n
                [keepalive_period_s=0..30]
                [keepalive_retries=1..10]
            [checksum=yes|no];
                [routing_domain=text];

                [add route]
                        net=x.x.x.x/n
                        [next_hop_site_name=text | gw_ip_addr=x.x.x.x]
                        [cost=n]
                        [service={conduit | internet | intranet | passthrough | local
| lan_gre_tunnel | discard | lan_ipsec_tunnel}]
                        [intranet_service_name=text]
                        [route_eligibility_based_on_path={yes | no}]
                        [route_eligibility_from_wan_link_name=text]
                        [route_eligibility_to_wan_link_name=text]
                        [route_eligible_on_gw={yes|no}]
                [route_eligible_on_tunnel={yes|no}]
                        [enable_export_to_other_sites={yes|no}];
                        [ipsec_tunne=text]
                        [routing_domain=text];

                add [identity_certificate|trusted_certificate]
                        name=[name]
                        fingerprint=[hex string]
```

```
                certificate=[base64 string modified to replace / with #]
                private_key=[base64 string modified to replace / with #]
                ;

        [add route_learning]
        {
                set ospf_properties
                        enabled=(yes|no)
                        [router_id=x.x.x.x]
                    [advertise_apn_routes=(yes|no)]
        [export_ospf_route_type=(type_1|type_5)]
        [export_ospf_route_weight=n]

                ;
                set bgp_properties
                        enabled=(yes|no)
                        local_as=1..4294967296
                        [router_id=x.x.x.x]
                        [advertise_apn_routes=(yes|no)]
                ;
                add ospf_area
                {
                        set ospf_area_properties
                                id=x.x.x.x or a number
                                [stub_area=(yes|no)]
                        ;
                        add ospf_area_virtual_interface
                                virtual_interface_name=name
                                [interface_cost=1..65535]
                                [password_type=(none|plain_text|md5)]
                                password=text
                                [hello_interval=1..65535]
                                [dead_interval=1..65535]
                        ;
                }
                add bgp_neighbor
                        virtual_interface_name=name
                        neighbor_ip_addr=x.x.x.x
                        password=text
                        [igp_metric=(yes|no)]
                        [hold_time=1..65535]
        [as_masquerade=number]
                        [local_preference=0..2147483647]
        [route_reflector_client=(yes|no)]
                        [next_hop_self=(yes|no)]

                ;
                add route_learning_filter
                        routing_domain=name
                        [source router ip addr=x.x.x.x]
```

```
                                    [destination_ip_addr=x.x.x.x]
                                    [destination_net_object_name=name]
                                    [route_prefix=[0..32 or *]
                                    [route_prefix_match_type=(eq|lt|le|gt|ge)]
                                    [next_hop_ip_addr=x.x.x.x]
                                    [protocol=(bgp|*|ospf)]
                                    [route_cost=1..65535 or *]
                                    [apn_cost=6..15]
                                    [include_route=(true|false)]
                                    [export_route=(true|false)]
                                    [route_eligible_on_gw=(true|false)]
                                    [route_eligibility_based_on_path=(true|false)]
                                    [route_eligibility_from_wan_link=name]
                                    [route_eligibility_to_wan_link=name]
                                    [route_cost_match_type=(eq|lt|le|gt|ge)]
                                    [service_type=(local|internet|intranet|conduit|lan_gre_tunn
                                el|lan_ipsec_tunnel|passthrough)]
                                    [service_name=name]
                                    [use_recursive_route=yes|no]
                                    [use_next_hop=yes|no]
                        [enabled={true|false}
                                ;
                          add route_learning_export_filter
                            routing_domain=name
                            [network_ip_addr=x.x.x.x]
                                [network_net_object_name=name]
                            [route_prefix=[0..32 or *]
                            [route_prefix_match_type=(eq|lt|le|gt|ge)]
                          [next_hop_ip_addr=x.x.x.x]
                          [apn_cost=1..16]
                          [include_route=(true|false)]
                          [route_cost_match_type=(eq|lt|le|gt|ge)
    [service_type=(local|internet|intranet|lan_gre_tunnel|lan_ipsec_tunnel|passthrough|ipho
        st|conduit or*)]
                          [service_name=name or*]
                          [enabled={true|false}
                          [export_ospf_route_type=(type_1|type_5)]
                          [export_ospf_route_weight=n]
                      ;
                }

                          add conduit_service remote_site_name=text //can be any site
                          {
                                  [set conduit_properties]
                                    [tracking_ip_addr=x.x.x.x]
                                    [reverse_also={yes | no}]
                                    [fallback_intranet_service_name=text]
                                    [unlink_default_set={yes | no}]
                                    [default_set_name=text];
```

```
                    [add path]
                        from_link=text
                        to_link=text
                        [tracking_ip_addr=x.x.x.x]
                        [reverse_also={yes | no}]
                        [reverse_tracking_ip_addr=x.x.x.x]
                        [enable_instability_sensitivity={yes | no}]
                        [enable_encryption={yes | no}]

        [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|c
s3|cs4|cs5|cs6|cs7|default|ef}]
                        [enable_bad_loss_sensitivity={yes | no}];
                [path_loss_threshold_pct=1..90]
                        [path_loss_threshold_over_time_ms=100..2000]
                        [silence_sensitivity_period_ms=150..1000]
                        [path_bad_to_good_probation_period_ms=500..60000];

                    [set realtime_class]
                        class_id=n
                        [class_name=text]
                        [initial_rate_kbps=n | initial_rate_pct=p ]
                        sustained_rate_kbps=n | sustained_rate_pct=p
                        [initial_period_ms=n];

                    [set interactive_class]
                        class_id=n
                        [class_name=text]
                        [initial_share_pct=p]
                        sustained_share_pct=p
                        [initial_period_ms=n];

                    [set bulk_class]
                        class_id=n
                        [class_name=text]
                        [bulk_share_pct=p];

                    [add rule]
                    {
                        [set properties]
                            [precedence={high | medium | low}]
                            [application_name=text]
                            [track_performance={yes | no}]
                            [override_service={passthrough | internet | intranet
| (intranet_name) | discard}] ;

                        set match_criteria
                    [application_match_name=text]
                            [ip_addrn=x.x.x.x/n]
                            [src_ip_addrn=x.x.x.x/n]
                            [dst ip addrn=x.x.x.x/n]
```

```
                                        [port_num=n-n]
                                        [src_port=n-n]
                                        [dst_port=n-n]
                                        [ip_protocol_num=n]

        [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|c
    s3|cs4|cs5|cs6|cs7|default|ef}]
                                        [ip_tos_match_flows={yes | no}]
                                        [rouing_domain=text]
                                        [vlan_id={native | 0...4094}]
                                        [protocol_str={ * | FTP | SMTP | HTTP | TELNET |
ICMP | HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

                                    [set traffic_optimization_properties]
                                        [enable_tcp_termination={yes | no}]
                                        [enable_wan_op={yes | no}]
                                        [other_header_compression_enabled={yes | no}]
                                        [gre_header_compression_enabled={yes | no}]
                                        [enable_packet_aggregation={yes | no}];

                                    [set ingress_properties]
                                        [class_id=n]
                                        [class_name=text]
                                        [class_tail_drop_small_packet_ms=n]
                                        [class_tail_drop_small_packet_bytes=n]
                                        [class_tail_drop_large_packet_size_bytes=n]
                                        [class_tail_drop_large_packet_ms=n]
                                        [class_tail_drop_large_packet_bytes=n]
                                        [class_dup_disable_depth_greater_ms=n]
                                        [class_dup_disable_depth_greater_bytes=n]

        [reassign_flow_if_packet_exceeds_size_bytes=n]

        [reassign_flow_if_packet_exceeds_size_class_id=n]

        [reassign_flow_if_packet_exceeds_size_class_name=text]
                                    [reassign_class_tail_drop_small_packet_ms=n]
                                        [reassign_class_tail_drop_small_packet_bytes=n]

        [reassign_class_tail_drop_large_packet_size_bytes=n]
                                        [reassign_class_tail_drop_large_packet_ms=n]
                                        [reassign_class_tail_drop_large_packet_bytes=n]

        [reassign_class_dup_disable_depth_greater_ms=n]

        [reassign_class_dup_disable_depth_greater_bytes=n]
                                        [tcp_standalone_ack_class_id=n]
                                        [tcp_standalone_ack_class_name=text]

        [tcp standalone ack class tail drop small packet ms=n]
```

```
        [tcp_standalone_ack_class_tail_drop_small_packet_bytes=n]

        [tcp_standalone_ack_class_tail_drop_large_packet_size_bytes=n]

        [tcp_standalone_ack_class_tail_drop_large_packet_ms=n]

        [tcp_standalone_ack_class_tail_drop_large_packet_bytes=n];

                                [set wan_properties]
                                        [transmit_mode={load_balance_paths |
duplicate_paths | persistent_path}]
                                        [retransmit_lost_packets={yes | no}];

                                [set egress_properties]
                                        [resequence_packets={yes | no}]
                                        [resequence_holdtime_ms=n]
                                        [discard_late_resequence_packets={yes | no}]

        [dscp_tag_value={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs
1|cs2|cs3|cs4|cs5|cs6|cs7|default|ef}];

                                        [set deep_packet_inspection_properties]
                                                [enable_passive_ftp_detection={yes | no}] ;
                                }
                        }

                        add internet_service
                        {
                                [set internet_properties]
                                      [primary_reclaim={yes | no}]
                                        [ignore_wan_link_status={yes | no}]
                                        [default_set_name=text]
                                        [export_default_routes={yes | no}];

                                [add rule]
                                {
                                        [set properties]
                                                [precedence={high | medium | low}]
                                                [application_name=text]
                                                [override_service={passthrough | intranet |
(intranet_name) | discard}];

                                                  set match_criteria
                                   [application_match_name=text]
                                                [ip_addrn=x.x.x.x/n]
                                                [src_ip_addrn=x.x.x.x/n]
                                                [dst_ip_addrn=x.x.x.x/n]
                                                [port_num=n-n]
                                                [ s r c _ p o r t = n - n ]
```

```
                                        [dst_port=n-n]
                                        [ip_protocol_num=n]

            [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|c
    s3|cs4|cs5|cs6|cs7|default|ef}]
                                        [ip_tos_match_flows={yes | no}]
                                        [rouing_domain=text]
                                        [vlan_id={native | 0...4094}]
                                        [protocol_str={ * | FTP | SMTP | HTTP | TELNET |
ICMP | HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

                                [set wan_properties]
                                        [wan_link_name=text];

                                [set deep_packet_inspection_properties]
                                        [enable_passive_ftp_detection={yes | no}] ;

                        }

                } // internet

                add intranet_service name=text
                {
                        [set intranet_properties]
                                [primary_reclaim={yes | no}]
                                [ignore_wan_link_status={yes | no}]
                                [default_set_name=text]
                                [routing_domain=text]
                [firewall_zone=text];

                        [add rule]
                        {
                                set properties
                                        [precedence={high | medium | low}]
                                        [application_name=text]
                                        [override_service={passthrough | internet |
    discard}];

                                set match_criteria
                           [application_match_name=text]
                                        [ip_addrn=x.x.x.x/n]
                                        [src_ip_addrn=x.x.x.x/n]
                                        [dst_ip_addrn=x.x.x.x/n]
                                        [port_num=n-n]
                                        [src_port=n-n]
                                        [dst_port=n-n]
                                        [ip_protocol_num=n]

            [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|c
    s3|cs4|cs5|cs6|cs7|default|ef}]
```

```
                                        [ip_tos_match_flows={yes | no}]
                                        [rouing_domain=text]
                                        [vlan_id={native | 0...4094}]
                                        [protocol_str={ * | FTP | SMTP | HTTP | TELNET |
ICMP | HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

                                [set deep_packet_inspection_properties]
                                        [enable_passive_ftp_detection={yes | no}] ;
                        }

                } // intranet

                add ipsec_tunnel
                 {
                        set ipsec_tunnel_properties
                                service_type = [intranet|lan|internet]
                                name = [name] //ignored when service_type = intranet
                                intranet_service_name = [name] //ignored when
    service_type = lan
                                routing_domain=[name]
                                local_tunnel_ip = [ip]
                                peer_tunnel_ip = [ip]
                                network_mtu = [576...1500]
                                ike_version = [ikev1|ikev2]
                                ike_mode = [main|aggressive]
                                ike_auth = [psk|cert]
                                ike_psk = [length 5 to 128 non-separator characters
    except: ' “ / < > { } ; & ] //ignore when ike_auth is not 'psk'
                                ike_cert = [name]
                                ike  peer  auth = [mirrored|psk|cert]
                                ike_peer_psk = [length 5 to 128 non-separator characters
    except: ' “ / < > { } ; & ] //ignore when ike_peer_auth is not 'psk' or ike_version is not
    'ikev2'
                                 ike_identity = [auto|ip_addr]
                                 ike_validate_peer_identity = [true|false]
                                 ike_dhgroup = [group1|group2|group5]
                                 ike_hash_algorithm = [md5|sha|sha256]
                                 ike_integ_algorithm = [md5|sha|sha256]
                                 ike_encryption_mode = [aes128|aes192|aes256]
                                 ike_lifetime_s = [0...86400]
                                 ike_lifetime_s_max = [0...86400]
                                 ike_dpd_s = [0...86400]
                                 ipsec_tunnel_mode = [tunnel]
                                 ipsec_type = [esp|esp_auth|ah|esp_null]
                                 ipsec_encryption_mode = [aes128|aes192|aes256]
                                 ipsec_pfsgroup = [none|group1|group2|group5]
                                 ipsec_hash_algorithm = [md5|sha|sha256]
                                 ipsec_lifetime_s = [0...86400]
                                 ipsec_lifetime_s_max = [0...86400] ipsec lifetime
                                 kb = [0...4194303]
```

```
                                        ipsec_lifetime_kb_max = [0...4194303]
                                    ipsec_network_mismatch =
        [drop|forward|skip_ipsec_routes]
                        keepalive=[yes|no]
                        firewall_zone=text
                                ;
                                add ipsec_protected_network
                                        source_network = [ip with prefix]
                                        destination_network = [ip with prefix]
                                ;
                                        }

                add firewall
                {
                        set firewall_properties
                                untracked_and_denied_timeout_seconds=n
                                tcp_initial_timeout_seconds=n
                                tcp_idle_timeout_seconds=n
                                tcp_closing_timeout_seconds=n
                                tcp_timewait_seconds=n
                                udp_initial_timeout_seconds=n
                                udp_idle_timeout_seconds=n
                                icmp_initial_timeout_seconds=n
                                icmp_idle_timeout_seconds=n
                                generic_initial_timeout_seconds=n
                                generic_idle_timeout_seconds=n
                                firewall_default_action={allow|drop} //if value is not set, use
setting from apn_properties
                                default_track_connection={yes|no} //if value is not set, use
setting from apn_properties
                                ;

                                // multiple site firewall policy templates can be added
                                // their order determines the order in which the policies from the
                                // templates will apply.
                                add site_firewall_policy_template
                                        name=Firewall_Template;
                                ;

                                add firewall_filter
                                {
                                        routing_domain=*|text

                                        //multiple from_zones may be defined
                                        add from_zone
                                                name=Firewall_Zone
                                        ;
                                        //multiple to_zones may be defined
                                        add to_zone
                                                name=Firewall Zone
```

```
                                        ;
                                application_match_name=text
                                        ip_protocol_num=n // n must lie within [0, 255]. default = 0

                src_service_type={local|conduit|lan_gre_tunnel|lan_ipsec_tunnel|intranet|internet}
                                        src_service_instance=text//Validity depends on
src_service_type, and whether firewall_filter is configured as part of a firewall_filter_set
                                        src_ip_addrn=*|x.x.x.x[/n]
                                        src_port=n|x-y

                dst_service_type={local|conduit|lan_gre_tunnel|lan_ipsec_tunnel|intranet|internet}
                                        dst_service_instance=text //Validity depends on
dst_service_type, and whether firewall_filter is configured as part of a firewall_filter_set
                                        dst_ip_addrn=*|x.x.x.x[/n]
                                        dst_port=n|x-y
                                        action={allow|drop|reject|count_and_continue}
                                        track_connection={yes|no} log_interval=n //n = [0,60-
                                        600]. default is 0, for no logging.
                                        log_connection_start={yes|no}
                                        log_connection_end={yes|no}
                                        allow_fragments={yes|no}
                                }

                                add static_nat_rule
                                {
                                        routing_domain=text//cannot specify wildcard
                                        direction={inbound|outbound}

                 service_type={local|conduit|lan_gre_tunnel|lan_ipsec_tunnel|intranet|internet}
                                        service_instance=text //depends on service_type.
                                        inside_zone=text
                                        inside_network_ip_addrn=x.x.x.x/n1 //n1 must be equal to n2
                                        outside_zone=text
                                        outside_network_ip_addrn=x.x.x.x/n2
                                }

                                add masq_nat_rule
                                {
                                        set masq_nat_rule_properties
                                                direction={inbound|outbound}
                                                type={port_restricted|symmetric}
                                                service_type={local|intranet|internet}
                                                service_instance=text //depends on
                                                service_type. inside_zone=text
                                                inside_network_ip_addrn=*|x.x.x.x/n
                                                outside_zone=text
                                                outside_network_ip_addr=x.x.x.x
                                                allow_related={yes|no}
                                                enable_ipsec_passthrough={yes|no}
                                                enable_gre_pptp_passthrough={yes|no}
```

```
                                        ;

                                            add port_forwarding_rule
                                    routing_domain=text
                                                inside_network_ip_addr=x.x.x.x
                                                protocol={tcp|udp|both}
                                                inside_port=n|x-y
                                                outside_port=n|x-y
                                                action={allow|drop|reject|count_and_continue}
                                                track_connection={yes|no|true|false}
                                                log_interval=n //n = [0,60-600]. default is 0, for no
logging.
                                                log_connection_start=z{yes|no}
                                                log_connection_end={yes|no}
                                                allow_fragments={yes|no}
                                        ;
                                }
                        }

                    add virtual_wan_link name=text
                            {
                                    add access_interface name=text
                                        virtual_interface_name=text
                                        virtual_ip_addr=x.x.x.x
                                        gw_ip_addr=x.x.x.x
                                        [enable_proxy_arp={yes | no}]
                                [enable_default_internet={yes|no}]
                                        [conduit_mode={primary|secondary|exclude}];

                                    set properties
                                        wan_ingress_physical_rate_kbps=n
                                        wan_egress_physical_rate_kbps=n
                                        [wan_ingress_permitted_rate_kbps=n]
                                        [wan_egress_permitted_rate_kbps=n]
                                        [access_type={public_internet | private_intranet
        |virtual_wan_link_container}]
                                        [mtu_bytes=n]
                                    [is_standby={yes | no}]
                                        [cell_size_bytes=n]
                                        [cell_hdr_bytes=n]
                                        [provider_id=n]
                                        [provider_link_frame_cost_bytes=n]
                                        [enable_public_ip_learning={yes | no}]
                                        [public_ip_addr=x.x.x.x]
                                        [tracking_ip_addr=x.x.x.x]
                                        [congestion_threshold_us_per_s_us=n]
                                        [wan_ingress_realtime_eligible={yes | no}]
                                        [wan_egress_realtime_eligible={yes | no}]
                                        [wan_ingress_interactive_eligible={yes | no}]
                                        [wan egress interactive eligible={yes | no}]
```

```
                                    [wan_ingress_bulk_eligible={yes | no}]
                                    [wan_egress_bulk_eligible={yes | no}]
                                    [wan_ingress_trigger_dynamic_conduit_rate_kbps=n]
                                    [wan_egress_trigger_dynamic_conduit_rate_kbps=n]
                                    [wan_ingress_trigger_dynamic_conduit_pps=n]
                                    [wan_egress_trigger_dynamic_conduit_pps=n]
                        [wan_ingress_permitted_rate_auto_learn={yes|no}]
                                [wan_egress_permitted_rate_auto_learn={yes|no}]
                                [wan_link_mode={regular_active|last_resort_standby
|on_demand_standby}]
                                [standby_wan_link_priority={1..3}]
                                [standby_wan_link_heartbeat_interval_s={0..10}]
                                [adaptive_bandwidth_detection={yes|no}]
                                [minimum_acceptable_bandwidth_for_abd_pct=p]
                        ;

                                [add service_group]
                                        name=text
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n;

                                add net_usage
                                        service_type={internet | intranet}
                                        [intranet_service_name=text]
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n
                                        [service_group_name=text]
                                        [use={primary | secondary | balance}]
                                        [max_delay_ms=n]
                                        [enable_wan_egress_grooming={yes | no}]
                                        [wan_ingress_dscp_tag_value=n]
                                        [wan_egress_dscp_match_value=n]
                                        [wan_egress_dscp_tag_value=n]
                                        [tunnel_hdr_size_bytes=n]
                                        [wan_ingress_minimum_reserved_bandwidth_kbps=n]
                                        [wan_egress_minimum_reserved_bandwidth_kbps=n]
                                        [wan_ingress_maximum_allowed_bandwidth_kbps=n]
                                        [wan_egress_maximum_allowed_bandwidth_kbps=n]
                                        [change_access_interface_upon_failure={yes|no}];

                                add conduit_usage
                                        remote_site_name=text
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n
                                        [service_group_name=text]
                                        [tunnel_hdr_size_bytes=n]
                                        [enable_udp_hole_punching={yes | no}]
                                        [active_path_mtu_discovery_enable={yes|no}]
                                        [udp_port_num=n]
                                        [udp_port_num_alt=n]
```

```
                                [udp_port_switch_interval_minutes=n]
                                [wan_egress_minimum_reserved_bandwidth_kbps=n]
                                [wan_ingress_minimum_reserved_bandwidth_kbps=n]
                                [wan_ingress_maximum_allowed_bandwidth_kbps=n]
                                [wan_egress_maximum_allowed_bandwidth_kbps=n]
                                [autopath_group_name=text];

                        add dynamic_conduit_usage
                                wan_ingress_rate_fair_share_for_all_dynamic_conduits=n
                                wan_egress_rate_fair_share_for_all_dynamic_conduits=n
                                [service_group_name=text]
                                [tunnel_hdr_size_bytes=n]
                                [enable_udp_hole_punching={yes | no}]
                                [active_path_mtu_discovery_enable={yes|no}]
                                [udp_port_num=n]
                                [udp_port_num_alt=n]
                                [udp_port_switch_interval_minutes=n]
                                [wan_egress_minimum_reserved_bandwidth_kbps=n]
                                [wan_ingress_minimum_reserved_bandwidth_kbps=n]
                                [wan_ingress_maximum_allowed_bandwidth_kbps=n]
                                [wan_egress_maximum_allowed_bandwidth_kbps=n]
                                [autopath_group_name=text];

                           add cos_wan_link name=text
                           {
                                set properties
                                        ip_dscp={<dscp tag>}
                                        [use_for_unmatched_tag={ yes | no}]
                                        wan_ingress_permitted_rate_kbps=n
                                        wan_egress_permitted_rate_kbps=n
                                        [tracking_ip_addr=x.x.x.x]
                                        [congestion_threshold_us_per_s_us=n]
                                        [wan_ingress_realtime_eligible={yes | no}]
                                        [wan_egress_realtime_eligible={yes | no} ]
                                        [wan_ingress_interactive_eligible={yes | no}]
                                        [wan_egress_interactive_eligible={yes | no} ]
                                        [wan_ingress_bulk_eligible={yes | no}]
                                        [wan_egress_bulk_eligible={yes | no} ]

        [wan_ingress_trigger_dynamic_conduit_rate_kbps=n ]

        [wan_egress_trigger_dynamic_conduit_rate_kbps=n ]
                                        [wan_ingress_trigger_dynamic_conduit_pps=n ]
                                        [wan_egress_trigger_dynamic_conduit_pps=n;]

                                [add service_group ]
                                        name=text
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n;
```

```
                                    add conduit_usage
                                        remote_site_name=text
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n
                                        [service_group_name=text]
                                        [tunnel_hdr_size_bytes=n]
                                        [enable_udp_hole_punching={yes | no} ]
                                        [active_path_mtu_discovery_enable={yes | no} ]
                                        [udp_port_num=n]
                                        [udp_port_num_alt=n]
                                        [udp_port_switch_interval_minutes=n]

            [wan_egress_minimum_reserved_bandwidth_kbps=n]

            [wan_ingress_minimum_reserved_bandwidth_kbps=n]

            [wan_egress_maximum_allowed_bandwidth_kbps=n]

            [wan_ingress_maximum_allowed_bandwidth_kbps=n]
                                        [autopath_group_name=text];

                                    add dynamic_conduit_usage

            wan_ingress_rate_fair_share_for_all_dynamic_conduits=n

            wan_egress_rate_fair_share_for_all_dynamic_conduits=n
                                        [service_group_name=text ]
                                        [tunnel_hdr_size_bytes=n]
                                        [enable_udp_hole_punching={yes | no} ]
                                        [active_path_mtu_discovery_enable={yes | no} ]
                                        [udp_port_num=n]
                                        [udp_port_num_alt=n]
                                        [udp_port_switch_interval_minutes=n]

            [wan_egress_minimum_reserved_bandwidth_kbps=n]

            [wan_ingress_minimum_reserved_bandwidth_kbps=n]

            [wan_egress_maximum_allowed_bandwidth_kbps=n]

            [wan_ingress_maximum_allowed_bandwidth_kbps=n]
                                        [autopath_group_name=Inherit];

                                    add net_usage
                                        service_type={intranet}
                                        intranet_service_name=text
                                        wan_ingress_rate_fair_share=n
                                        wan_egress_rate_fair_share=n
                                        [use={primary | secondary}]
                                        [service_group_name=text]
```

```
                                        [max_delay_ms=n]
                                        [enable_wan_egress_grooming={yes  |  no}  ]
                                        [wan_egress_dscp_tag_value={<dscp tag > |
 Inherit}]
                                        [tunnel_hdr_size_bytes=n]
        [wan_egress_minimum_reserved_bandwidth_kbps=n]
        [wan_ingress_minimum_reserved_bandwidth_kbps=n]
        [wan_egress_maximum_allowed_bandwidth_kbps=n]
        [wan_ingress_maximum_allowed_bandwidth_kbps=n];
                        }
                }
        }

        [add ha_appliance]
                name=text;

        [add ha_service]
        {
                set properties
                        primary_appliance_name=text
                        secondary_appliance_name=text
                        [failover_ms=n]
                        [primary_reclaim={yes | no}]
                        [shared_mac=xx:xx:xx:xx:xx:xx]
                        [use_serial_ha={yes | no}];

                add interface_group //NOTE: “add ha_interface_group” also accepted
here.
                {
                        set interface_properties
                                virtual_interface_name=text
                                primary_ip_addr=x.x.x.x
                                secondary_ip_addr=x.x.x.x;

                        [add external_tracker]
                                ip_addr=x.x.x.x;
                }
        }
 } // site
 [define wan_to_wan_forwarding_group name=text ]
 {

 }
```

```
        [set apn_properties]
                [encryption_mode={aes128|aes256}]
                [encryption_rekey_enabled={yes|no}]
                [enhanced_message_authentication={yes|no}]
                [enhanced_message_authentication_type={checksum|sha256}]
                [enhanced_packet_uniqueness={yes|no}]
                [firewall_default_action={allow|drop}]
                [firewall_policy_template_name=text]
                [default_track_connection={yes|no}]
                        [path_bandwidth_test_time_ms=n]
                        [compiler_version=text]
        ;

        define firewall_zone
              name=Firewall_Zone
        {
        //presently, no attributes or sub-objects are defined
}

define firewall_policy_template
        name=Firewall_Template
{
        add pre_appliance_policies
        {
                //these rules will be inserted in the registry before an appliance's static and
automatic policies
                add firewall_filter... //multiple filters may be added, see definition under site ->
appliance -> firewall
        }
        add post_appliance_policies
        {
             //these rules will be inserted in the registry after an appliance's static and
automatic policies
                add firewall_filter...
        }
}
          [define application name=text]
        {
              set application_properties
                    [gather_mos={true|false}];
        }
        define application_category name=text
        {
                set application_category_properties
                [talari_defined=true|false]
                ;
        }
define application_match_collection
{
      [define application match name=text]
```

```
    {
        set application_properties
            [enabled={yes|no}]
                        [application_category=text]
                          [application_classification=text]
                       [probing_interval_s={0|10|60|120|300}]
                       [response_time_normal_ms=[2-1000]]
                      [response_time_warning_ms=[2-2000]]
            ;
        add application_match_criteria
            [ip_addrn1=x.x.x.x/n]
                        [ip_addrn2=x.x.x.x/n]
                        [port_num1=n-n]
                        [port_num2=n-n]
            [domain_name=text]
                        [ip_protocol_num=n]
      [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs6|cs7|default|ef}]
                    ;
      }
}
define site_group_object name=text
{
       add application_site
            site_name=text
            ;
}

add application_policy name=text
{
            set application_policy_properties
                [enabled={yes|no}]
                [routing_domain=text]
                [destination_site=text]
                [destination_service=text]
                [classification=text]
                ;

            add application_category_match
                application_category=text
                ;
            add application__name_match
                application_match_name=text
                ;
            add source_network_match
                source_network_name=text
                ;
            add site_group_match
                site_group_name=text
                ;
```

```
                    add site_match
                            site_name=text
}
[define autopath_group name=text]
          {
                set autopath_group_properties
                     [enable_encryption={yes|no}]
                     [enable_instability_sensitivity={yes|no}]
                     [enable_bad_loss_sensitivity={yes|no}]
                     [path_loss_threshold_pct=1..90]
                     [path_loss_threshold_over_time_ms=100..2000]
                     [silence_sensitivity_period_ms=150..1000]
                     [path_bad_to_good_probation_period_ms=500..60000]
                     [is_default={yes|no}]

          [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|c
          s5|cs6|cs7|default|ef};
          }
          [define routing_domain name=text]
          {
                 set routing_domain_properties


                    [is_default={yes|no}] ;
          }
          define net_object
                name=text
          {
                add network
                      ip_addrn=x.x.x.x/n
                ;
          }
 [define dhcp_option_set name=text]
{
          [add dhcp_option]
                    [is_option={yes|no}]

     option_name={vendor_encapsulated_options|netbios_name_servers|netbios_node_typ
e|tftp_server_name|tftp_server_address|ip_telephone|custom|max_lease_time |
default_lease_time | subnet_mask | routers | domain_name_servers |domain_name}
                    option_number={1| 3| 6| 15| 43 | 44 | 46 | 66 | 150 | 176 | 224 - 254}
                    value=[This depends on the user specified data_type option]
                    data_type={string|integer|ip_address|domain_name}
          ;
          }
          define dynamic_conduit_default_set name=text
          {
                set advanced_properties
                    [activate_standby_bandwidth_threshold_percentage=1..200]
          ;
```

```
        set ipsec_properties
                enabled = [yes|no]
                tunnel_type = [esp|esp_auth|ah]
                encryption_mode = [aes128|aes256]
                hash_algorithm = [sha|sha256]
                lifetime_s = [0...86400];
        [set realtime_class]
                class_id=n
                [initial_rate_pct=p]
                sustained_rate_pct=p
                [initial_period_ms=n] ;

        [set interactive_class]
                class_id=n
                [initial_share_pct=p]
                sustained_share_pct=p
                [initial_period_ms=n] ;

        [set bulk_class]
                class_id=n
                [bulk_share_pct=p]
                [delay_min_depth_bytes=n];

        [set dynamic_conduit_properties]
            [create_conduit_sampling_time_seconds=n]
            [create_conduit_wan_ingress_min_throughput_rate_kbps=n]
            [create_conduit_wan_egress_min_throughput_rate_kbps=n]
            [create_conduit_wan_ingress_min_pps=n]
            [create_conduit_wan_egress_min_pps=n]
            [remove_conduit_sampling_time_minutes=n]
            [remove_conduit_wan_ingress_througput_rate_kbps=n]
            [remove_conduit_wan_egress_througput_rate_kbps=n]
            [remove_conduit_wan_ingress_pps=n]
            [remove_conduit_wan_egress_pps=n]
            [remove_conduit_down_wait_time_minutes=n]
            [recreate_conduit_hold_time_minutes=n]

        [add rule]
    {
            [set properties]
                [precedence={high | medium | low}]
                [application_name=text]
                [track_performance={yes | no}]

            set match_criteria
                [application_match_name=text]
                [ip_addrn=x.x.x.x/n]
                [src_ip_addrn=x.x.x.x/n]
                [dst_ip_addrn=x.x.x.x/n]
                [port_num=n-n]
```

```
                [src_port=n-n]
                [dst_port=n-n]
                [ip_protocol_num=n]
                [ip_dscp=aaxx]
                [ip_tos_match_flows={yes | no}]
                [rouing_domain=text]
                [vlan_id={native | 0...4094}]
                [protocol_str={ * | FTP | SMTP | HTTP | TELNET | ICMP | HTTPS | SSH |
RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];
        [set traffic_optimization_properties]
                [enable_tcp_termination={yes | no}]
                [enable_wan_op={yes | no}]
                [enable_packet_aggregation={yes | no}];

        [set ingress_properties]
                [class_id=n]
                [class_name=text]
                [class_tail_drop_small_packet_ms=n]
                [class_tail_drop_small_packet_bytes=n]
                [class_tail_drop_large_packet_size_bytes=n]
                [class_tail_drop_packet_ms=n]
                [class_tail_drop_packet_bytes=n]
                [class_dup_disable_depth_greater_ms=n]
                [class_dup_disable_depth_greater_bytes=n]
                [reassign_flow_if_packet_exceeds_size_bytes=n]
                [reassign_flow_if_packet_exceeds_size_class_id=n]
                [reassign_flow_if_packet_exceeds_size_class_name=text]
[               [reassign_class_tail_drop_small_packet_ms=n]
                [reassign_class_tail_drop_small_packet_bytes=n]
                [reassign_class_tail_drop_large_packet_size_bytes=n]
                [reassign_class_tail_drop_packet_ms=n]
                [reassign_class_tail_drop_packet_bytes=n]
                [reassign_class_dup_disable_depth_greater_ms=n]
                [reassign_class_dup_disable_depth_greater_bytes=n]
                [tcp_standalone_ack_class_id=n]
                [tcp_standalone_ack_class_name=text]
[               [tcp_standalone_ack_class_tail_drop_small_packet_ms=n]
                [tcp_standalone_ack_class_tail_drop_small_packet_bytes=n]
               [tcp_standalone_ack_class_tail_drop_large_packet_size_bytes=n]
               [tcp_standalone_ack_class_tail_drop_packet_ms=n]
               [tcp_standalone_ack_class_tail_drop_packet_bytes=n];

         set wan_properties
                [transmit_mode={load_balance_paths | duplicate_paths | persistent_path}]
                [preferred_wan_link_name=text]
                [persistent_path_impedance_ms=n]
                [retransmit_lost_packets={yes | no}];

         set egress_properties
                [resequence packets={yes | no}]
```

```
                    [resequence_holdtime_ms=n]
                    [discard_late_resequence_packets={yes | no}]
                    [dscp_tag_value=aaxx];

                [set deep_packet_inspection_properties]
                    [enable_passive_ftp_detection={yes | no}] ;
                }
        }
        define service_provider name=text
            add wan_link_template name=text
        {
            set wan_link_template_properties
                link_type={broadband|private_link|mpls}
                wan_ingress_physical_rate_kbps=1000000
                wan_egress_physical_rate_kbps=1000000
                wan_ingress_permitted_rate_auto_learn=false
                wan_egress_permitted_rate_auto_learn=false
                autopath_group_name=encrypted_Autopath_Group
            ;
        }
add wan_link_template_mpls_queue

        [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|cs3|cs4|cs5|cs
default|ef}]
                        wan_ingress_permitted_rate_kbps=n
                        wan_egress_permitted_rate_kbps=n
                    }
}
```

Formatting Note: For a particular parameter, some of the entries have a value contained in parentheses to the right of the parameter's name. This value is the default or recommended setting for that parameter. For the parameter entry, default_direct_route_cost = Number (5), "5" would be the default setting for default_direct_route_cost. If a particular parameter has no value listed after the parameter name, it can be assumed that there is no default setting for that parameter.

Commands and Parameters

define site

Keyword	Type	Description	Required	Default
name	Text	The name of the site.	Yes	N/A

add appliance

Keyword	Type	Description	Required	Default
name	Text	The name of the appliance.	Yes	N/A

set appliance_properties

Keyword	Type	Description	Required	Default
secure_key	Hex Number	Up to 64 of the 128 bits (16 hex digits) in the AES encryption key used by the service. The two sites in a conduit have their keys concatenated together and use this composite key to encrypt and decrypt traffic.	Yes	N/A
model	Text	The model of the APN Appliance, used to verify that interfaces are used correctly in interface groups.	Yes	N/A
license	Text	The type of license for the appliance. Each appliance has its own set of valid license types defined in platform_descriptions.xml. The valid values for this parameter is dependent upon the hardware model. T510: unlimited T730: unlimited T750: unlimited T860: h_200 | l_100 | unlimited T3000: l_240 | h_500 | unlimited T3010: l_300 | h_500 | unlimited T5000: l_1000 | h_3000 | unlimited T5200: h_3000 | unlimited VT500: h_40 | unlimited **VT800: "no_license" | 20 | 40 | 100 | 200 |** unlimited | custom CT800: h_100 | unlimited	No	**"unlimited"**

Keyword	Type	Description	Required	Default
license_rate	Number	The licensed rate of the appliance specified in Mbps. Valid range depends on the appliance model where the value must be 0 for the T510, T730, and T750 models and between the following ranges for the higher models: T860: 1-200 T3000: 1-500 T3010: 1-500 T5000: 1-3000 T5200: 1-3000 VT500: 1-40 VT800: 1-200 CT800: 1-100 This field is only configurable by the user in the instance that the “license” parameter is set to “custom”. Otherwise, this value is set to the number specified in the “license” parameter. (Example: “l_100” sets this value as “100”). Otherwise, if the “license” param is set to “unlimited”, then this rate is set to “0”, and no ingress/egress permitted WAN Link rates are checked against this number.	No	0
appliance_mode	Text	Specifies the appliance's role in the APN. It can be set as “primary_ncn”, “secondary_ncn”, or “client”.	No	“client”
enable_src_mac_learning	Boolean	(Added for 2.5P2) MAC address learning is a service that stores the source MAC address of each received packet so that future packets destined for that address can be forwarded only to that port on which that address is located. Packets destined for unrecognized addresses are forwarded out every port.	No	no
enable_wan_to_wan_forwarding	Boolean	If set, this indicates that this site will be used as a proxy for Mutli-Hop APN traffic	No	no
wan_to_wan_forwarding_route_cost	Number	The route cost that will be advertised for Multi-Hop routes that travel through this appliance. This cost must be between 1 and 15. Lower cost routes will be preferred over higher cost routes.	No	10
default_direct_route_cost	Number	The default route cost that will be used for routes added on this appliance. This cost must be between 1 and 15. Lower cost routes will be preferred over higher cost routes.	No	5
is_intermediate_site	Boolean	If this flag is enabled for a site, then that site will be used as an intermediate site for use in creating dynamic conduits between two sites. If a site is flagged as being an intermediate site, it must have enable_wan_to_wan_forwarding enabled, and must have a static conduit defined to all sites where dynamic conduits are configured.	No	No

Keyword	Type	Description	Required	Default
wan_to_wan_forwarding_group	Cour	When configuring wan_to_wan forwarding or dynamic conduits, setting this string will ensure that wan_to_wan routes or dynamic conduits will only be created between this site, and other sites that have wan_to_wan_forwarding_group specified. (example, setting this parameter to the string “west_coast” will mean that dynamic conduits or wan_to_wan routes will only be created to other sites where the wan_to_wan_forwarding_group=”west_coast”)	No	N/A
persist_ucast_refresh_time_ms	Number	The number of milliseconds between the Talari Appliance ARP requests for configured gateway IP addresses	No	1000
max_dynamic_conduits_for_site	Number	Maximum number of dynamic conduits allowed to be established between this site and any other qualified site. APN Appliance model already has a maximum allowed, hence this optional parameter if set will limit the max allowed for this site to a value less than the maximum allowed for this APN model.	No	
enable_conduit_to_conduit_forwarding	Boolean	If set, this site will forward traffic received from one conduit to another conduit. Unlike enable_wan_to_wan_forwarding, it will not advertise multi-hop routes to other sites.	No	No
enable_conduit_to_ii_forwarding	Boolean	If set, this site will forward traffic received from conduit to internet/intranet, it will also forward traffic received from internet/intranet to conduit. Unlike enable_wan_to_wan_forwarding, it will not advertise this site's intenet/intranet routes to other sites.	No	No

add interface_group

set properties

Keyword	Type	Description	Required	Default
secure_zone	Text	Determines whether the interface group is on a trusted (such as behind a firewall) or untrusted (such as wan aux) segment	No	Trusted
bypass_mode	Text	If the ports in the interface group form a bypass pair, setting this to “fail_to_wire” will cause the interfaces to go into bypass mode when the Talari service is not running	Yes, if there are >= 2 interfaces in interface_group	fail_to_block

Keyword	Type	Description	Required	Default
Is_bridged	Boolean	If this flag is enabled, any user defined bridge pairs will be ignored, and bridge pairs will be automatically created by the compiler for ethernet interfaces in the interface group that form hardware bypass pairs. **NOTE: No audits will be implemented to check for pre-existing bypass pairs, nor will this field be visible in the advanced panel, as this was created to simplify a feature in the simplified configuration editor.**	No	No

add bridge_pair

Keyword	Type	Description	Required	Default
device_one	Text	The name of the first device to be used in this bridge_pair. Must correspond to an ethernet interface used within this interface group.	Yes	N/A
device_two	Text	The name of the second device to be used in this bridge_pair. Must correspond to an ethernet interface used within this interface group.	Yes	N/A
is_port_state_reflection_enabled	Boolean	If enabled, the link state of the devices in the bridge pair are in synchronization. If the link state of device_one goes down, then device_two goes down, and vice-versa. If the link_state comes back up for device_one, then device_two will come back up, and vice-versa.	No	No

add ethernet_interface

Keyword	Type	Description	Required	Default
device	Text	The name (from the appliance silkscreen) of an ethernet device in this interface group. Note that in Release 2.1, we will accept the names from the “old” silkscreens (WAN, LAN, etc), however all listing files will contain the new names to match the new appliance silkscreens, statistics and the APN Graphical Configuration editor.	Yes	N/A

add virtual_interface

Keyword	Type	Description	Required	Default
name	Text	The name to be used when referencing this virtual interface through the configuration and user interfaces.	Yes	N/A
is_dhcp_client	Boolean	Determines the mode of DHCP in which this virtual interface will operate. Choices are currently restricted to “true” or “false”. Setting this value to “false” implies that a user must provide their own static virtual IP Addresses for this virtual interface (this was the previous behavior for virtual interfaces). Setting this value to “true” will make the WAN Link Access Interface specifying this Virtual Interface obtain its Virtual IP and Gateway information via DHCP.	No	No
routing_domain	Text	This is the routing_domain that this virtual interface is associated with. Only traffic sourced/destined for the specified routing_domain may utilize this interface.	No	“”
vlan_id	Number	The VLAN ID to be used for identifying and marking traffic to and from this VLAN	No	0
firewall_zone	Text	The Firewall Zone for the VLAN.	No	Default_LAN_Zone

add virtual_ip_addrn

Keyword	Type	Description	Required	Default
virtual_interface_name	Text	The name of the virtual interface that this ip_addrn is associated with.	Yes	N/A
ip_addrn	Network Address	A valid local IP used for arping on the subnet designated by the given prefix.	Yes	N/A
is_identity	Boolean	If enabled, this IP address will be used for IP services such as BGP and OSPF.	No	False

Keyword	Type	Description	Required	Default
is_private	Boolean	If enabled, the Virtual IP Address will only be routable on the local Appliance.	No	False

add site_routing_domain

Keyword	Type	Description	Required	Default
Name	String	This is the name of a routing_domain that is defined at the network level, that is being used by this site's objects.	Yes	N/A
is_default	Boolean	Setting this will enable this routing domain as default at site.	No	False

add route

Keyword	Type	Description	Required	Default
net	Network Address	This subnet will be used in the forwarding information database. Packets destined to this subnet will be directed to the given service.	Yes	N/A
gw_ip_addr	IP Address	If the route service is not conduit, internet or intranet, this is the IP address of the gateway that packets will be directed to.	Yes, if service is not conduit, internet, intranet or discard	N/A
next_hop_site_name	Text	If the route service is conduit, this is the remote site of the conduit that packets will be directed to.	Yes, if service =conduit	N/A
cost	Number	The route cost for this route. This cost must be between 1 and 15. Lower cost routes will be preferred over higher cost routes.	No	5
service	Text	The service for this route.	No	local
intranet_service_name	Text	Name of intranet service to be used for this route	Yes, if service_type=intranet	N/A
route_eligibility_based_on_path	Boolean	Enable the route failover feature – route eligibility will be based on the state of an associated path NOTE: The restriction of this parameter as an intranet only route parameter was lifted as of the GA release of 4.1	No	N/A
route_eligibility_from_wan_link_name	Text	The 'from' WAN link name for the path that determines whether or not to mark this route as ineligible based on the state of the specified path.	No	N/A
route_eligibility_to_wan_link_name	Text	The 'to' WAN link name for the path that determines whether or not to mark this route as ineligible based on the state of the specified path.	No	N/A

Keyword	Type	Description	Required	Default
route_eligible_on_gw	Boolean	Enabling this option will cause a route to only be valid if the gateway specified in this route is reachable. For use in local routes only	No	No
enable_export_to_other_sites	Boolean	Setting this flag to “no” will ensure that this route will never be used when establishing wan_to_wan or dynamic conduit routes to other remote sites. For use in internet/intranet routes only.	No	Yes
ipsec_tunnel	Text	This is the LAN IPSec Tunnel the route is referencing. This is only applicable in the event that the route's service type is set to “lan_ipsec_tunnel or internet.”	Yes, if service_type=lan_ipsec_tunnel	N/A
routing_domain	Text	This is the routing_domain that this route is associated with. Only traffic sourced/destined for the specified routing_domain may utilize this interface.	No	“”
route_eligible_on_turnnel	Boolean	Enabling this option will cause a route to only be valid if the tunnel specified in this route is up. For use in LAN IPsec, Intranet IPsec or Internet IPsec routes only.	No	No

add route_learning

set ospf_properties

Keyword	Type	Description	Required	Default
enabled	Boolean	Setting this will enable route learning using OSPF.	Yes	False
router_id	IP Address	The IP address that will be used as the router id when advertising routes using OSPF	No	N/A
advertise_apn_routes	Boolean	Setting this will advertise routes from the APN route table via ospf	No	False
export_ospf_route_type	Text	When Bird export routes learned from APN to other OSPF neighbors, it can export the route either type_1 or type_5.	No	type_5
export_ospf_route_weight	Number	When Bird export routes learned from APN to other OSPF neighbors, the cost of the route will be this weight plus original APN cost.Supported range: 0-65529.	No	0

set bgp_properties

Keyword	Type	Description	Required	Default
enabled	Boolean	Setting this flag will enable route learning using BGP.	Yes	true

Keyword	Type	Description	Required	Default
local_as	Number	BGP configuration local AS number 1.. 4294967296. If this is enabled, the local AS number must be set by the user.	No	N/A
router_id	IP Address	The IP address that will be used as the router id when advertising this site to BGP neighbors	No	N/A
advertise_apn_routes	Boolean	Setting this will advertise routes from the APN route table via bgp		false

set ospf_area_properties

Keyword	Type	Description	Required	Default
id	IP Address or Number	Identification for the OSPF area. This can be either an IP Address or a Number	Yes	N/A
stub_area	Boolean	Configure the OSPF area as a stub area to avoid flooding of external routes.	No	no

add ospf_area_virtual_interface

Keyword	Type	Description	Required	Default
virtual_interface_name	text	Name of the Talari Virtual Interface that belongs to the configured area.	Yes	N/A
interface_cost	number	The base cost for routes learned on the interface	No	10
password_type	text	Authentication type used for the OSPF password.	No	md5
password	text	Password used for authentication for the OSPF session.	No	N/A
hello_interval	number	Time in seconds between sending of Hello messages.	No	10
dead_interval	number	Elapsed time in seconds before declaring the neighbor down	No	40

add bgp_neighbor

Keyword	Type	Description	Required	Default
virtual_interface_name	text	Name of the Talari Virtual Interface that belongs to the BGP neighbor.	Yes	N/A
neighbor_ip_addr	IP Address	IP Address identifying the BGP neighbor.	Yes	N/A
password	text	Password used for md5 authentication of the BGP session	Yes	N/A
igp_metric	Boolean	If this is set, then the internal distances will be used to calculate the best route.	No	yes

Keyword	Type	Description	Required	Default
hold_time	number	Specify the hold-time value to use when negotiating a connection with the peer. The hold-time value is advertised in open packets and indicates to the peer the length of time that it should consider the sender valid. If the peer does not receive a keepalive, update, or notification message within the specified hold time, the BGP connection to the peer is closed and routing devices through that peer become unavailable.(1..65535)	No	180
local_preference	number	BGP Local Preference setting which is a metric used by BGP sessions to indicate the degree of preference for an external route. The route with the highest local preference value is preferred. The LOCAL_PREF path attribute always is used in inbound routing policy and is advertised to internal BGP peers and to neighboring confederations. It is never advertised to external BGP peers. – (0..4294957295)	No	100
as_masquerade	Number	BGP configuration AS masquerade number 1..2147483647	No	Same as local_as
remote_as	Number	BGP configuration remote AS number 1..2147483647	No	Same as local_as
route_reflector_client	Boolean	If enabled, neighbor will be treated as a route reflector client.	No	No
next_hop_self	Boolean	If enabled, add “next hop self” in BGP config file	No	yes
disable_loop_protection	Boolean	If enabled, local AS loop protection is disabled.	No	no

add route_learning_filter

Keyword	Type	Description	Required	Default
routing_domain	Text	The name of the routing domain to match the correct routing table when multi-mode is being used for this site.	Yes	N/A
source_router_ip_addr	IP Address	IP address of the source router	No	*
destination_ip_addr	IP Address	IP address destination network for which the filter is applied	No	*
destination_net_object_name	text	Destination network object for which the filter is applied.	No	*
route_prefix	Number	Route prefix value to match/compare to, using the route prefix match type operator	No	*

Keyword	Type	Description	Required	Default
route_prefix_match_type	Text	Operator used when comparing route prefix (eq, le, lt, ge, gt)	No	Eq
next_hop_ip_addr	Text	Next Hop IP address	No	*
protocol	text	Select the dynamic routing protocol for filtering routes. (bgp, *, ospf)	No	*
route_cost	Number	Route cost value to match/compare to, using the route_cost_match_type operator.	No	*
apn_cost	number	(6..15)	No	6
route_tag	Number	0..4294967295	No	*
include_route	Boolean	Include the route if it matches the filter	No	Yes
export_route	Boolean	Export route to remote sites (yes or no) (This value is not enforced based on the service_type. It will be ignored when not applicable.)	No	Yes
route_eligible_on_gw	Boolean	If enabled, the rout will not receive traffic when the gateway is unreachable.	No	Yes
route_eligibility_based_on_path	Boolean	If enabled, the route will not receive traffic when the selected path is down.	No	Yes
route_eligibility_from_wan_link	Text	The 'from' WAN link name for the path that determines whether or not to mark this route as ineligible based on the state of the specified path.		N/A
route_eligibility_to_wan_ink	Text	The 'to' WAN link name for the path that determines whether or not to mark this route as ineligible based on the state of the specified path.		N/A
route_cost_match_type	Text	Operator used when comparing route costs (eq, le, lt, ge, gt)	No	Eq
service_type	Text	Select the talari service type for the route to filter on. This can be (local, intranet, internet, conduit, lan_gre_tunnel, lan_ipsec_tunnel, passthrough)	No	local
service_name	Text	Name of the service specified in the service_type if it is one of conduit, intranet, lan_gre_tunnel, lan_ipsec_tunnel. (Ignored when service_type is local, internet, passthrough)	No	N/A
use_recursive_route	Boolean	Ignored if service type is not conduit. If enabled, service_name is ignored. APN will find the service name based on import route's source router.	No	No

Keyword	Type	Description	Required	Default
use_next_hop	Boolean	Only used when recursive route is enabled. If enabled, recursive route will use next hop of the route to find the conduit. If disabled, recursive route will use source router of the route to find the conduit.	No	No
Enabled	Boolean	Setting enabled=false causes this filter to have no effect.	No	Yes

add route_learning_export_filter

Keyword	Type	Description	Required	Default
routing_domain	Text	The name of the routing domain to match the correct routing table when multi-mode is being used for this site.	No	*
network_ip_addr	IP Address	IP address destination network for which the filter is applied.	No	*
network_net_object_name	Text	Destination network object for which the filter is applied.	No	*
route_prefix	Number	Route prefix value to match/compare to, using the route_prefix_match_type operator.	No	*
route_prefix_match_type	Text	Operator used when comparing route prefix (eq, le, lt, ge, gt).	No	eq
next_hop_ip_addr	IP Address	The IP address of the gateway	No	*
apn_cost	Number	(1..16)	No	*
include_route	Boolean	Include the route if it matches the filter.	No	false
apn_cost_match_type	Text	Operator used when comparing route costs (eq, le, lt, ge, gt).	No	eq
service_type	Text	Select the Talari service type of the route to filter on. This can be (local|internet|intranet|lan_gre_tunnel|lan_ipsec tunnel|any|iphost|conduit|*).	No	*
service_name	Text	Name of the service specified in the service_type if it is one of intranet, lan_gre_tunnel, lan_ipsec_tunnel or conduit. (Ignored when service_type is local, internet, any, *).	No	any/*
Enabled	Boolean	Setting enabled=false causes the filter to have no effect.	No	Yes
export_ospf_route_type	Text	When Bird export routes learned from APN to other OSPF neighbors, it can export the route either type_1 or type_5.	No	type_5
export_ospf_route_weight	Number	When Bird export routes learned from APN to other OSPF neighbors, the cost of the route will be this weight plus original APN cost.	No	0

add dynamic_conduit_service

Keyword	Type	Description	Required	Default
name	Text	This is the name of the dynamic_conduit_default_set used to define the conduit properties for this site for any dynamic conduits created involving this site.	Yes	N/A

add identity_certificate | trusted_certificate

Keyword	Type	Description	Required	Default
name	Text	Name of the certificate	Yes	N/A
fingerprint	Text	Fingerprint to uniquely identify the certificate – generated by the compiler and written to the configuration file. (This value is not validated, nor is it required to be provided by [...])	No	N/A
certificate	Text (large)	Defines the certificate with a Base64 string with '/' characters replaced with '#' characters.	Yes	none
private_key	Text (large)	Defines the private key with a Base64 string with '/' characters replaced with '#' characters. This is used when generating an identity_certificate and not used when generating a trusted_certificate.	Yes if identity_certificate	none

add conduit_service

set conduit_properties

Keyword	Type	Description	Required	Default
tracking_ip_addr	IP Address	The virtual IP that will be correlated with the state of this conduit, allowing it be tracked via ping.	No	N/A
reverse_also	Boolean	If this conduit should be automatically created in the reverse direction. If not, must be explicitly defined at both sites. If TRUE, rules and classes are created in both directions. If FALSE, rules and classes are only created for the site where the conduit is defined.	No	yes
default_set_name	Text	Name of the set of conduit defaults that will be used to populate rules and classes.	No	N/A

Keyword	Type	Description	Required	Default
unlink_default_set	Boolean	When a Conduit Default Set Name is set for the conduit service and unlink_default_set param is yes, then the Conduit Default Set Classes and the Conduit Classes will be merged together and marked as Unlinked from Conduit Default Set for the Classes. After this the changes applied to Conduit Default Set Classes will not be reflected in the Conduit Service Classes.	No	no

add path

Keyword	Type	Description	Required	Default
from_link	Text	Indicates the origination WAN link of the path.	Yes	N/A
to_link	Text	Indicates the destination WAN link of the path.	Yes	N/A
tracking_ip_addr	IP Address	The virtual IP that will be correlated with the state of this path, allowing it be tracked via ping.	No	N/A
reverse_also	Boolean	Indicates that the a path between the same WAN links but in the opposite direction should be added.	No	yes
reverse_tracking_ip_addr	IP Address	The virtual IP that will be correlated with the state of the auto configured reverse path, allowing it be tracked via ping.	No	N/A
enable_instability_sensitivity	Boolean	If set to no, high loss will not cause the path to go BAD. This is useful if a path has significantly more bandwidth than the others and avoiding the path due to high loss would cause intolerable loss of bandwidth.	No	yes
enable_encryption	Boolean	Indicates whether packets that are sent along this path should be encrypted.	No	yes
ip_dscp	Text	Permits the user to set a dscp tag in the IP header for path traffic. The user may configure the down stream router to use these fields to do DSCP routing for the paths to ensure unique paths through the network.	No	N/A
enable_bad_loss_sensitivity	Boolean	If set to no, instability will not cause the path to go BAD. This is useful if a path has significantly more bandwidth than the others and avoiding the path due to instability would cause intolerable loss of bandwidth.	No	Yes

Keyword	Type	Description	Required	Default
path_loss_threshold_pct	Number	Percentage threshold before path is considered bad. This threshold is measured over specified time. When this field is not specified, the default is to measure packet loss based on the last received 200 packets. Valid value are 1-90%	No	N/A
path_loss_threshold_over_time_ms	Number	Specify sample period over which to evaluate packet loss. Used in conjunction with path_loss_threshold_pct. Valid values are 100-2000ms	No	1000
silence_sensitivity_period_ms	Number	Specify silence duration before Path state transitions from GOOD to BAD. Valid values are 150-1000ms	No	150ms
path_bad_to_good_probation_period_ms_is_set	Number	Specify the probation period to wait before moving Path state transitions from BAD to GOOD. Valid values are 500-60000ms	No	10000

set realtime_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<class_id>
initial_rate_kbps	Number	Defines the maximum initial rate in kbps that this class may consume while the queue depth is less than initial period ms.	No	initial_rate_pct
initial_rate_pct	Percent	Defines the maximum initial rate in as a percentage of the conduit total bandwidth that this class may consume while the queue depth is less than initial period ms.	No	initial_rate_kbps
sustained_rate_kbps	Number	Defines the rate this class may consume of the conduit bandwidth in kbps if queue_depth is > initial_period_ms.	No	sustained_rate_pct
sustained_rate_pct	Percent	Defines the rate this class will use of the conduit bandwidth as a percent share of the entire conduit.	No	sustained_rate_kbps
initial_period_ms	Number	Defines the queue depth at which switch is made between initial_rate and sustained_rate.	No	0

set interactive_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<class id>

Keyword	Type	Description	Required	Default
initial_share_pct	Percent	Defines the maximum initial rate in as a percentage of the conduit total bandwidth that this class may consume while the queue depth is less than initial_period_ms.	No	sustained_share_pct
sustained_share_pct	Percent	Defines the rate this class will use of the conduit bandwidth as a percent share of the entire conduit.	Yes	N/A
initial_period_ms	Number	Defines the queue depth at which switch is made between initial_rate and sustained_rate. This parameter must be set to the same value for all interactive classes defined in the conduit. (For Talari defined default classes, this value will be set automatically to the value used by the other user defined classes.)	No	0

set bulk_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<class id>
bulk_share_pct	Percent	Percentage of the all the bulk classes' share of the conduit bandwidth that this class will use.	No	1

add rule

set properties

Keyword	Type	Description	Required	Default
precedence	Text	Provides up to three sets of rules that will be scanned in priority order. First match found is taken. Order of rules is priority and then listed order in the config. All high priorities will be scanned, in the order listed, then mediums and then lows. There is no best match, only first match; so for example, more generalized IP networks (/32) should be placed in the low priority and last in order in order to allow more specific matches to take.	No	low
application_name	Text	A name given to a rule that will allow rule statistics to be summed in groups when they are displayed. All rule statistics for rules with the same application_name can be viewed together.	No	N/A

Keyword	Type	Description	Required	Default
track_performance	Boolean	If yes, performance of a rule over time will be recorded in a session DB including loss, latency, jitter and bandwidth used.	No	no
override_service	Text	The destination service that flows of this type should go to.	No	N/A

set match_criteria

Keyword	Type	Description	Required	Default
ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed. If either source or destination matches this, then rule is hit.	No	N/A
src_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
dst_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
port_num	Range	If set, if either the destination or source port matches this number, the packet will hit the rule.	No	N/A
src_port	Range	If set, if the source port matches this number, the packet will hit the rule.	No	N/A
dst_port	Range	If set, if the destination port matches this number, the packet will hit the rule.	No	N/A
ip_protocol_num	Number	Defines an explicit protocol number as is set in the packets IP protocol field in the IP header.	No	N/A
ip_dscp	Text	Defines an explicit DSCP tag as is set in IP protocol fields in the IP header.	No	N/A
ip_tos_match_flows	Boolean	If set to YES, ip_tos will be included as a criterion for creating new flows.	No	No
protocol_str	Text	Defines protocol that the filter will match. In particular, this rule represents the protocol type bits in the TCP header or the IP header as well as common ports for this protocol.	No	N/A
routing_domain	Text	This is the routing domain that this rule will match. If the user sets this to a specific domain, only traffic on that domain will be eligible to match this rule. If the user chooses not to set this value, ALL domains are eligible to match this domain.	No	N/A
vlan_id	Number	This is the VLAN ID that this rule will match. If the user sets this parameter to number (0-4096) only traffic tagged with that VLAN ID will be considered eligible to match this rule. Otherwise, if the user does not set this value, ALL	No	N/A

Keyword	Type	Description	Required	Default
		VLAN IDs are eligible to match this rule.		
application_match_name	Text	The application_match object that a packet must match for this rule. Note: If this field is set, IP address, port, protocol and dscp match settings for this rule will not be used in matching this rule.	No	N/A

set traffic_optimization_properties

Keyword	Type	Description	Required	Default
enable_tcp_termination	Number	This parameter is used to enable or disable the TCP Termination feature on this (TCP-based) rule.	No	No
enable_wan_op	Boolean	This parameter is used to enable or disable the WAN Optimization feature on this (TCP-based) rule. Supported models: T5200, T5000, T3010, E100, VT800, CT800.	No	No
other_header_compression_enabled	Boolean	If true, the we will perform header compression. If false, we should not. Applicable to IP, UDP, TCP headers.	No	No
gre_header_compression_enabled	Boolean	If true, we should perform GRE header compression. If false, we should not. Only supported when protocol is GRE or 47.	No	Yes for GRE, no for any other rule
enable_packet_aggregation	Boolean	If true, we should aggregate conduit user packet data packets that match this rule. If false, we should not aggregate packets that match this rule	No	no

Note: When transferring files using FTP or SCP with TCP termination enabled, the reported rate of transfer is the rate between local client machine and local APNA. Since TCP termination buffers numerous TCP packets and acknowledges incoming packets locally, the transfer rate can be much higher than the user's WAN link bandwidth. The transfer is reported complete only when all the packets are sent to the destination and acknowledgement is received. Therefore, there may be some delay between seeing a message that the files are 100% sent and the transfer actually being complete.

set ingress_properties

Keyword	Type	Description	Required	Default
class_id	Number	Defines the class number that is to service traffic flows that match this rule.	One and only one of these two parameters must be set.	N/A
class_name	Text	Defines the class name that is to service traffic flows that match this rule.		N/A
class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than "class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted. This value must be <= 1500.	No, not valid for bulk classes (automatically reverted to 0)	IF REFERENCING INTERACTIVE CLASS: if conduit bandwidth < 4000 Mbps, default = Largest realtime class_tail_drop_small_packet_ms value + 70, else default = Largest realtime class_tail_drop_small_packet_ms value + 150 OTHERWISE: 50
class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than "class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
class_tail_drop_large_packet_size_bytes	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop policy. If n=0, all packets treated as small packets. This value must be <= 1500.	No	0
class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to "class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes	0

Keyword	Type	Description	Required	Default
class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	0
class_dup_disable_depth_greater_ms	Number	Designates the amount of time a duplicate packet may wait in the queue before being discarded, which prevents duplicate packets from consuming bandwidth when bandwidth is limited.	No	greater of class_tail_drop_small_packet_ms and class_tail_drop_large_packet_ms
class_dup_disable_depth_greater_bytes	Number	Defines the queue depth of the class scheduler at which point duplicate packets will begin being discarded.	No	IF REFERENCING A BULK CLASS: if conduit bandwidth > 4000 Mbps, default = total conduit bandwidth * 25 ms, else default = conduit bandwidth * 75/2 ms OTHERWISE: 128000
reassign_flow_if_packet_exceeds_size_bytes	Number	After a flow is established, if a packet that exceeds this size is detected on WAN ingress, then the flow will be moved to the class indicated below.	Only required if reassign_flow_if_packet_exceeds_size_class_id or reassign_flow_if_packet_exceeds_size_class_name is set.	2000
reassign_flow_if_packet_exceeds_size_class id	Number	The class id of the class to which flows will be reassigned if the size above is exceed.	One and only one of these two parameters must be set if reassign_flow_if_packet_exceeds_size_bytes is set.	N/A
reassign_flow_if_packet_exceeds_size_class_name	Text	The class name of the class to which flows will be reassigned if the size above is exceed.		N/A

Keyword	Type	Description	Required	Default
reassign_class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than "reassign_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes (automatically reverted to 0)	IF REFERENCING INTERACTIVE CLASS: if conduit bandwidth < 4000 Mbps, default = Largest realtime reassign_class_tail_drop_small_packet_ms value + 70, else default = that Largest realtime reassign_class_tail_drop_small_packet_ms value + 150 OTHERWISE: 50
reassign_class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than "reassign_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
reassign_class_tail_drop_large_packet_size_bytes	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop policy. If n=0, all packets treated as small packets. This value must be <= 1500.	No	0
reassign_class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to "reassign_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes	0

Keyword	Type	Description	Required	Default
reassign_class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "reassign_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	0
reassign_class_dup_disable_depth_greater_ms	Number	Designates the amount of time a duplicate packet may wait in the queue before being discarded, which prevents duplicate packets from consuming bandwidth when bandwidth is limited.	No	greater of reassign_class_tail_drop_small_packet_ms and reassign_class_tail_drop_large_packet_ms
reassign_class_dup_disable_depth_greater_bytes	Number	Defines the queue depth of the class scheduler at which point duplicate packets will begin being discarded.	No	IF REFERENCING A BULK CLASS: if conduit bandwidth > 4000 Mbps, default=total conduit bandwidth * 25 ms, else default=conduit bandwidth * 75/2 ms OTHERWISE: 128000
tcp_standalone_ack_class_id	Number	The class id of the class that will be used for standalone TCP ACKs. This has no effect on packets that are piggyback ACKs with payload.	No	class_id
tcp_standalone_ack_class_name	Text	The class name of the class that will be used for standalone TCP ACKs. This has no effect on packets that are piggyback ACKs with payload.	No	N/A

Keyword	Type	Description	Required	Default
tcp_standalone_ack_class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes (automatically reverted to 0)	IF REFERENCING INTERACTIVE CLASS: if conduit bandwidth < 4000 Mbps, default = Largest realtime tcp_standalone_ack_class_tail_drop_small_packet_ms value + 70), else default = Largest realtime tcp_standalone_ack_class_tail_drop_small_packet_ms value + 150 OTHERWISE: 50
tcp_standalone_ack_class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
tcp_standalone_ack_class_tail_drop_large_packet_size_bytes	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop policy. If n=0, all packets treated as small packets. This value must be <= 1500.	No	0
tcp_standalone_ack_class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes	0

Keyword	Type	Description	Required	Default
tcp_standalone_ack_class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	0

set wan_properties

Keyword	Type	Description	Required	Default
transmit_mode	Text	Select from the three available methods of transferring packets: Load balancing across multiple paths, duplicating across the two most unique paths, sending on a single persistent path.	No	load_balance_paths
preferred_wan_link_name	Text	Only applies when transmit mode is persistent path. User defines the WAN Link that should be used first when picking a path for the packets hitting this rule.	No	N/A
persistent_path_impedance_ms	Number	Only applies when transmit mode is persistent path. User defineds how much backup on the path before moving to another path. Valid range: 5-1000	No	50
retransmit_lost_packets	Boolean	This parameter specifies that flows matching this rule will be sent using reliable service to the remote appliance, and as such that any packets lost will be retransmitted.	No	no

set egress_properties

Keyword	Type	Description	Required	Default
resequence_packets	Boolean	Defines that traffic flows that match this rule should be tagged for sequence order, and the packets should be reordered (if necessary) at the WAN Egress appliance.	No	no
resequence_holdtime_ms	Number	Defines the maximum delay that a packet may be held awaiting re-sequence. When the timer expires the packet will be sent to the LAN without waiting any further for the pre-requisite sequence numbers.	No	If TCP: 900 If Non-TCP: 250
discard_late_resequence_packets	Boolean	After a packet's sequence timer has expired for a dependent packet, and the packets were permitted to the LAN: If a late packet does arrives at WAN egress, this property defines what is to be done with it.	No	Yes

Keyword	Type	Description	Required	Default
dscp_tag_value	Text	Defines a dscp tag that will be applied to packets that match this rule on WAN egress, before they are sent to the LAN.	No	N/A

set deep_packet_inspection_properties

Keyword	Type	Description	Required	Default
enable_passive_ftp_detection	Boolean	If enabled, will make processing decisions based upon user data.	No	Non-FTP rule->NO FTP rule->YES

add internet_service

set internet_properties

Keyword	Type	Description	Required	Default
primary_reclaim	Boolean	If set, the (use=primary) internet usage associated with this service on a WAN Link will forcefully reclaim as the active service on that WAN Link	No	yes
export_default_routes	Boolean	If this flag is enabled, the default route created for this internet service (0.0.0.0/0) will be exported to remote sites when this internet service's site is configured for WAN to WAN Forwarding.	no	yes
ignore_wan_link_status	Boolean	If set, packets destined for the Internet service will still pick the Internet route if all the WAN Links associated with this Internet service are down.	No	no
default_set_name	Text	Name of the set of Internet defaults that will be used to populate rules.	No	N/A

add rule

set properties

Keyword	Type	Description	Required	Default
precedence	Text	Provides up to three sets of rules that will be scanned in priority order. First match found is taken. Order of rules is priority and then listed order in the config. All high priorities will be scanned, in the order listed, then mediums and then lows. There is no best match, only first match; so for example, more generalized IP networks (/32) should be placed in the low priority and last in order in order to allow more specific matches to take.	No	low
application_name	Text	A name given to a rule that will allow rule statistics to be summed in groups when they are displayed. All rule statistics for rules with the same application_name can be viewed together.	No	N/A
override_service	Text	The destination service that flows of this type should go to.	No	N/A

set match_criteria

Keyword	Type	Description	Required	Default
application_match_name	Text	The application_match object that a packet must match for this rule. Note: If this field is set, IP address, port, protocol and dscp match settings for this rule will not be used in matching this rule.	No	N/A
ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed. If either source or destination matches this, then rule is hit.	No	N/A
src_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
dst_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
port_num	Range	If set, if either the destination or source port matches this number, the packet will hit the rule.	No	N/A
src_port	Range	If set, if the source port matches this number, the packet will hit the rule.	No	N/A
dst_port	Range	If set, if the destination port matches this number, the packet will hit the rule.	No	N/A
ip_protocol_num	Number	Defines an explicit protocol number as is set in the packets IP protocol field in the IP header.	No	N/A
ip_dscp	Text	Defines an explicit DSCP tag as is set in IP protocol fields in the IP header.	No	N/A
ip_tos_match_flows	Boolean	If set to YES, ip_tos will be included as a criterion for creating new flows.	No	No
protocol_str	Text	Defines protocol that the filter will match. In particular, this rule represents the protocol type bits in the TCP header or the IP header as well as common ports for this protocol.	No	N/A
routing_domain	Text	This is the routing domain that this rule will match. If the user sets this to a specific domain, only traffic on that domain will be eligible to match this rule. If the user chooses not to set this value, ALL domains are eligible to match this domain.	No	N/A
vlan_id	Number	This is the VLAN ID that this rule will match. If the user sets this parameter to number (0-4096) only traffic tagged with that VLAN ID will be considered eligible to match this rule. Otherwise, if the user does not set this value, ALL VLAN IDs are eligible to match this rule.	No	N/A

set wan_properties

Keyword	Type	Description	Required	Default
wan_link_name	Text	If wan_link name provided and internet load balancing is being used, flow will use the specified WAN link and not one automatically chosen by load balancing.	No	N/A

set deep_packet_inspection_properties

Keyword	Type	Description	Required	Default
enable_passive_ftp_detection	Boolean	If enabled, will make processing decisions based upon user data.	No	Non-FTP rule->NO FTP rule->YES

add intranet_service

set intranet_properties

Keyword	Type	Description	Required	Default
primary_reclaim	Boolean	If set, the (use=primary) intranet usage associated with this service on a WAN Link will forcefully reclaim as the active service on that WAN Link	No	yes
ignore_wan_link_status	Boolean	If set, packets destined for the Internet service will still pick the Internet route if all the WAN Links associated with this Internet service are down.	No	no
default_set_name	Text	Name of the set of Intranet defaults that will be used to populate rules.	No	N/A
routing_domain	Text	This is the routing_domain that this intranet service is associated with. Only traffic sourced/destined for the specified routing_domain may utilize this intranet service.	No	“”
firewall_zone	Text	The Firewall Zonw for the Service.	No	Default_LAN_Zone

add rule

set properties

Keyword	Type	Description	Required	Default
precedence	Text	Provides up to three sets of rules that will be scanned in priority order. First match found is taken. Order of rules is priority and then listed order in the config. All high priorities will be scanned, in the order listed, then mediums and then lows. There is no best match, only first match; so for example, more generalized IP networks (/32) should be placed in the low priority and last in order in order to allow more specific matches to take.	No	low
application_name	Text	A name given to a rule that will allow rule statistics to be summed in groups when they are displayed. All rule statistics for rules with the same application_name can be viewed together.	No	N/A
override_service	Text	The destination service that flows of this type should go to.	No	N/A

set match_criteria

Keyword	Type	Description	Required	Default
application_match_name	Text	The application_match object that a packet must match for this rule. Note: If this field is set, IP address, port, protocol and dscp match settings for this rule will not be used in matching this rule.	No	N/A
ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed. If either source or destination matches this, then rule is hit.	No	N/A
src_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
dst_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
port_num	Range	If set, if either the destination or source port matches this number, the packet will hit the rule.	No	N/A
src_port	Range	If set, if the source port matches this number, the packet will hit the rule.	No	N/A
dst_port	Range	If set, if the destination port matches this number, the packet will hit the rule.	No	N/A

Keyword	Type	Description	Required	Default
ip_protocol_num	Number	Defines an explicit protocol number as is set in the packets IP protocol field in the IP header.	No	N/A
ip_dscp	Text	Defines an explicit DSCP tag as is set in IP protocol fields in the IP header.	No	N/A
ip_tos_match_flows	Boolean	If set to YES, ip_tos will be included as a criterion for creating new flows.	No	No
protocol_str	Text	Defines protocol that the filter will match. In particular, this rule represents the protocol type bits in the TCP header or the IP header as well as common ports for this protocol.	No	N/A
routing_domain	Text	This is the routing domain that this rule will match. If the user sets this to a specific domain, only traffic on that domain will be eligible to match this rule. If the user chooses not to set this value, ALL domains are eligible to match this domain.	No	N/A
vlan_id	Number	This is the VLAN ID that this rule will match. If the user sets this parameter to number (0-4096) only traffic tagged with that VLAN ID will be considered eligible to match this rule. Otherwise, if the user does not set this value, ALL VLAN IDs are eligible to match this rule.	No	N/A

set deep_packet_inspection_properties

Keyword	Type	Description	Required	Default
enable_passive_ftp_detection	Boolean	If enabled, will make processing decisions based upon user data.	No	Non-FTP rule->NO FTP rule->YES

add ipsec_tunnel

set ipsec_tunnel_properties

Keyword	Type	Description	Required	Default
service_type	Text	Type of service this tunnel is associated with – intranet (associated with a specific Intranet service) - lan – (unassociated with any service – bypasses WAN Link/Service scheduling) - internet (associated with Zscaler) - internet_pa (associated with Palo Alto)	No	Intranet
name	Text	Name of the tunnel – used when service_type == lan	Yes if service_type = lan	N/A

Keyword	Type	Description	Required	Default
intranet_service_name	Text	Name of the intranet service this tunnel is associated with – used when service_type == intranet	Yes if service_type = intranet	N/A
local_tunnel_ip	IP Address	IP address defining the local tunnel – selected from the VIPs for the local site.	Yes	N/A
peer_tunnel_ip	IP Address	IP addresss defining the remote side of the tunnel.	Yes	N/A
network_mtu	Number	The maximum packet size for IKE and IPsec packets. Valid values are 576-1500	No	1500
routing_domain	Text	Name of the routing domain this tunnel is associated with	Yes	Default_RoutingDomain
ike version	Text	Defines the IKE version to use (1 or 2)	No	ikev1
ike_mode	Text	Defines the mode IKE will use (main or aggressive)	No	main
ike_auth	Text	Defines the authentication method to use (Pre Shared Keys, or Certificates) (psk|cert)	No	psk
ike_psk	Text	Defines the Pre Shared Key for this site if using ike_auth=PSK. This is a string of up to 128 characters NOTE: The compiler only checks or uses the ike_psk value only when ike auth=psk	Yes if ike_auth = psk	N/A
ike_cert	Text	Defines the name of the Certificate if using ike_auth=cert.	Yes if ike_auth = cert	N/A
ike_peer_auth	Text	Defines the authentication used on the peer – mirrored (same as the local), Pre-Shared Key or Certificate. (mirrored|psk|cert)	No	mirrored
ike_peer_psk	Text	Defines the Pre Shared Key for the peer site. If the ike_peer_auth is psk, or ike_peer_auth is mirrored and ike_auth is also psk. This is a string of up to 128 characters. NOTE: The compiler only checks or uses the ike_peer_psk value only when the ike_version=ike2 and ike_peer_auth=psk Note: Minimum of 5 chars is required.	Yes if ike_version =ikev2 and ike_peer_auth=psk	N/A
ike_identity	Text	Defines how the peer identity is made (auto or IP address) (auto|ip addr)	No	auto
ike_validate_peer_identity	Boolean	Defines whether or not to validate the peer identity.	No	true
ike_dhgroup	Text	Defines the Diffie-Hellman group to use in the key exchange process of setting up the tunnel. (group1|group2|group5)	No	group2
ike_hash_algorithm	Text	Defines the IKE hash algorithm to use. (md5|sha|sha256)	No	sha

Keyword	Type	Description	Required	Default
ike_integ_algorithm	Text	Defines the IKE integrity algorithm to use. (md5|sha|sha256)	No	sha
ike_encryption_mode	Text	Defines the IKE encryption mode to use. (aes128|aes192|aes256)	No	aes128
ike_lifetime_s	Number	Defines the lifetime (in seconds) of the keys for Phase 1. Valid values are 0-86400.	No	3600
ike_lifetime_s_max	Number	Defines the maximum lifetime (in seconds) of the keys for Phase 1. Valid values are 0-86400.	No	86400
ike_dpd_s	Number	Defines the time (in seconds) to wait before declaring a peer dead when no messages or DPD responses have been received. Valid values are 0-86400.	No	300
ipsec_tunnel_mode	Text	Defines the tunnel mode to use. Presently, only tunnel mode is supported.	No	tunnel
ipsec_type	Text	Defines the protocol used (Encapsulating Security Payloads, ESP, ESP+Auth, AH or ESP-NULL)	No	ESP for Intranet; ESP-NULL for Zscaler; ESP+AUTH for Palo Alto
ipsec_encryption_mode	Text	Defines the IPSEC encryption mode to use. (aes128|aes192|aes256) Not applicable for ipsec-type esp-null	No	aes128
ipsec_hash_algorithm	Text	Defines the IPSEC hash algorithm to user. (md5|sha|sha256)	No	sha
ipsec_lifetime_s	Number	Defines the lifetime (in seconds) of the keys for ipsec (phase 2). Valid values are 0-86400.	No	28800
ipsec_lifetime_s_max	Number	Defines the maximum lifetime (in seconds) of the keys for ipsec (phase 2). Valid values are 0-86400.	No	86400
ipsec_lifetime_kb	Number	Defines the lifetime of an ipsec tunnel as the number of kb transferred – the tunnel is taken down when this limit is reached and re-negotiated. Valid values are 0-4194303.	No	0
ipsec_lifetime_kb_max	Number	Defines the lifetime maximum number of kb that the site will accept when negotiating a tunnel with a remote site. Valid values are 0-4194303.	No	0
ipsec_network_mismatch	Text	Defines how Network/Policy mismatch behavior is managed – either (drop, forward, or skip ipsec routes).	No	drop
firewall_zone	Text	The Firewall Zone for the tunnel – used when service type is LAN. Inferred from the Intranet Service, otherwise.	No	Default_LAN_Zone

Keyword	Type	Description	Required	Default
keepalive	Boolean	Enables or disables keepalive for the tunnel. If enabled, the tunnel will be kept active whenever possible and all routes for the tunnel will have eligibility enabled.	No	No

add ipsec_protected_network

Keyword	Type	Description	Required	Default
source_network	Network Address	Source Network IP address / prefix – describing a network allowed to use the tunnel.	Yes	N/A
destination_network	Network Address	Destination Network IP address / prefix – describing a network allowed to use the tunne.	Yes	N/A

add firewall

set firewall_properties

Keyword	Type	Description	Required	Default
untracked_and_denied_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing Untracked or Denied Connections.	No	30
tcp_initial_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing a TCP session that has not completed a handshake.	No	120
tcp_idle_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing an active TCP session.	No	7440
tcp_closing_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing a TCP session after a request to terminate.	No	60
tcp_timewait_seconds	Integer	The time, in seconds, to wait for new packets before closing a terminated TCP session.	No	120

Keyword	Type	Description	Required	Default
udp_initial_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing a UDP session that has not seen traffic in both directions.	No	30
udp_idle_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing an active UDP session.	No	300
icmp_initial_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing an ICMP session that has not seen traffic in both directions.	No	30
icmp_idle_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing an active ICMP session.	No	60
generic_initial_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing a generic session that has not seen traffic in both directions.	No	30
generic_idle_timeout_seconds	Integer	The time, in seconds, to wait for new packets before closing an active generic session.	No	300
firewall_default_action	Text	The action for packets the do not match a policy.	No	Whatever value was set in apn_properties globally
default_track_connection	Boolean	Whether or not Connection state tracking is enabled for packets that do not match a policy.	No	Whatever value was set in apn_properties globally

add site_firewall_policy_template

Keyword	Type	Description	Required	Default
name	Text	The name of the firwall template being added to this site. The order in which these appear determines the order in which the pre and post policies of each template will be applied to the site's firewall fitlers collection.	yes	N/A

add firewall_filter

set firewall_filter_properties

Keyword	Type	Description	Required	Default
routing_domain	Text	The Routing Domain this Filter will apply to.	No	*
application_match_name	Text	The application_match object that a packet must match for this rule. Note: If this field is set, IP address, port, protocol and dscp match settings for this rule will not be used in matching this rule.	No	N/A
ip_protocol_num	Integer	The IP Protocol that the Filter will match.	No	0
src_service_type	Text	The Source Service Type that the Filter will match.	No	Any
src_service_instance	Text	The Source Service that the Filter will match.	No	*
src_ip_addrn	Network Address	The Source IP Address and Subnet Mask that the Filter will match.	No	*
src_port	Range	The Source Port or Port Range that the Filter will match.	No	0-65535
dst_service_type	Text	The Destination Service Type that the Filter will match.	No	Any
dst_service_instance	Text	The Destination Service that the Filter will match.	No	*
dst_ip_addrn	Network Address	The Destination IP Address and Subnet Mask that the Filter will match.	No	*
dst_port	Range	The Destination Port or Port Range that the Filter will match.	No	0-65535
action	Text	The Action to take for each packet matching the Filter.	No	allow
track_connection	Boolean	Enables or disables Connection state tracking for traffic matching the filter.	No	Not-set. An unset value infers the value set in firewall_properties.

Keyword	Type	Description	Required	Default
log_interval	Integer	The time, in seconds, between logging the number of packets matching the filter (0 = disabled, valid settings are 60-600).	No	0
log_connection_start	Boolean	Enables or disables logging when a new Connection is created by a packet matching this Filter.	No	No
log_connection_end	Boolean	Enables or disables logging when a Connection matching this Filter is deleted.	No	No
allow_fragments	Boolean	Enables or disables filtering of fragments when the action is allow.	No	Yes

add from_zone

Keyword	Type	Description	Required	Default
name	Text	This is the name of the Policy Template defined globally whose filters will be included in this site's collection of firewall filters.	Yes	N/A

add to_zone

Keyword	Type	Description	Required	Default
name			Yes	N/A

add static_nat_rule

Keyword	Type	Description	Required	Default
routing_domain	Text	Routing Domain this translation will apply to.	No	N/A
direction	Text	The direction, from the Service or Virtual Interface perspective, the translation will operate.	Yes	outbound
service_type	Text	The Service Type that the translation applies to.	Yes	N/A
service_instance	Text	The Service Name that the translation applies to.	Yes	N/A

Keyword	Type	Description	Required	Default
inside_zone	Text	The Zone a packet must be from to allow translation.	Yes (if outbound)	N/A
inside_network_ip_addrn	Network Address	The Inside IP Address and Subnet Mask to translate (Source IP Address in the direction selected).	Yes	N/A
outside_zone	Text	The Zone a packet must be destined for to allow translation.	Yes (if inbound)	N/A
outside_network_ip_addrn	Network Address	The Outside IP Address and Subnet Mask packets will be translated to (Source IP Address in the direction selected).	Yes	N/A

add masq_nat_rule

set masq_nat_rule_properties

Keyword	Type	Description	Required	Default
direction	Text	The direction, from the Service or Virtual Interface perspective, the translation will operate.	No	outbound
type	Text	The type of Dynamic NAT to perform.	No	port_restricted
service_type	Text	The Service Type that the translation applies to.	Yes	N/A
service_instance	Text	The Service Name that the translation applies to.	Yes	N/A
inside_zone	Text	The Zone a packet must be from to allow translation.	No	""
inside_network_ip_addrn	Network Address	The Inside IP Address and Subnet Mask to translate (Source IP Address in the direction selected).	Yes	N/A
outside_zone	Text	The Zone a packet must be destined for to allow translation.	No	Any
outside_network_ip_addr	IP Address	The Outside IP Address packets will be translated to (Source IP Address in the direction selected).	Yes	N/A

Keyword	Type	Description	Required	Default
allow_related	Boolean	If enabled, packets related to the Connection will be allowed (ICMP error packets).	No	No
enable_ipsec_passthrough	Boolean	If enabled, IPsec AH and ESP traffic will be translated. Only a single session from the inside network will be permitted.	No	No
enable_gre_pptp_passthrough	Boolean	If enabled, GRE/PPTP traffic will be translated. Only a single session from the inside network will be permitted.	No	No

add port_forwarding_rule

Keyword	Type	Description	Required	Default
routing_domain	Text	Routing Domain this Rule will match.	For masq_nat_rules on Internet Service only	N/A
inside_network_ip_addr	IP Address	The Inside IP address to forward to.	Yes	N/A
protocol	Text	The IP protocol to forward (TCP, UDP, both)	No	both
inside_port	Range	The Inside port or port range to forward to. If a range is configured, it must define the name number of ports as the outside_port.	No	N/A
outside_port	Range	The Outside port or port range to forward.	No	N/A
track_connection	Boolean	Enables or disables Connection state tracking for traffic matching the rule.	No	Not-set. An unset value infers the value set in firewall_properties.
log_interval	Integer	The time, in seconds, between logging the number of packets matching the rule (0 = disabled, valid settings are 60-600).	No	0

Keyword	Type	Description	Required	Default
log_connection_start	Boolean	Enables or disables logging when a new Connection is created by a packet matching this rule.	No	No
log_connection_end	Boolean	Enables or disables logging when a Connection matching this rule is deleted.	No	No
allow_fragments	Boolean	Enables or disables filtering of fragments.	No	Yes

add virtual_wan_link

add access_interface

Keyword	Type	Description	Required	Default
virtual_interface_name	Text	The virtual interface that this access interface will use to communicate.	Yes	N/A
virtual_ip_addr	IP Address	IP address for the talari endpoint to the WAN.	Yes	N/A
gw_ip_addr	IP Address	IP address for the gateway router.	Yes	N/A
enable_proxy_arp	Boolean	Indicates whether proxy arp will be enabled for this wan link. If other links share the same gw_ip_addr as this link, both links must have the same setting for this parameter. Cannot enable this parameter if the link interfaces an interface group that is not overlay (has less than 2 ethernet interfaces)	No	No
enable_default_internet	Boolean	Indicates whether this access interface will be used to provide access to the Internet service for all routing domains.	No	No
conduit_mode	Text	Denotes whether this access_interface will be used as a primary access_interface for conduit traffic, secondary access_interface for conduit traffic, or not used for conduit traffic. Options are “primary”, “secondary” or “exclude”.	no	“primary”

set properties

Keyword	Type	Description	Required	Default
wan_ingress_physical rate kbps	Number	RAW Bit Rate on the wire the of the WAN link for WAN ingress traffic	Yes	N/A
wan_egress_physical_ rate kbps	Number	RAW Bit Rate on the wire the of the WAN link for WAN egress traffic	Yes	N/A

Keyword	Type	Description	Required	Default
wan_ingress_permitted_rate_kbps	Number	Available rate of the WAN link for WAN ingress traffic	No	wan_ingress_physical_rate_kbps
wan_egress_permitted_rate_kbps	Number	Available rate of the WAN link for WAN egress traffic. If over 98% of the value of wan_egress_physical_rate_kbps, the compiler will adjust the value of wan_egress_perm itted_rate_kbps back down to 98% when writing out the registry file.	No	wan_egress_physical_rate_kbps
access_type	Text	Indicates if the WAN link is connected to a private IP network or to the public Internet. If the access type is "private_intranet_container", then this virtual_wan_link will contain separate "cos_wan_link" objects, representing the separate class of services available for an MPLS service.	No	public_internet
mtu_bytes	Number	largest raw packet size (Ethernet is 1518) (does not include any provider link frame cost bytes).	No	1500
cell_size_bytes	Number	Size of a cell including cell header overhead; payload can be calculated by subtracting cell hdr bytes.	No	N/A
cell hdr bytes	Number	Size of any cell overhead.	No	N/A
provider_id	Number	Designates that this WAN link belongs to the same service provider as any other WAN link with the same service provider id.	No	(unique value)
provider_link_frame_cost_bytes	Number	Bytes of header and trailers that are added in addition to every packet for the WAN link when transmitted. MTU should count these. Example may be Ethernet IPG of 160 bits, or AAL5 trailers.	No	0
enable_public_ip_learning	Boolean	Indicates whether the Talari should automatically detect the public P address.	No	no
public_ip_addr	IP Address	IP address of the Network Address Translator or proxy server	No	N/A
tracking_ip_addr	IP Address	The virtual IP that will be correlated with the state of this wan link, allowing it be tracked via ping. This parameter is not valid from the scope of a link where access type=virtual wan link container.	No	N/A
congestion_threshold_us_per_s_us	Number	The number of microseconds per second of congestion that must be detected on a WAN link before it goes into congestion avoidance mode. This parameters is not valid from the scope of a where access_type=virtual_wan_link_container.	No	20000

Keyword	Type	Description	Required	Default
wan_ingress_realtime_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified WAN link as their local WAN link will not be used for realtime traffic unless no other path is up. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Yes
wan_egress_realtime_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified WAN link as their remote WAN link will not be used for realtime traffic unless no other path is up. This parameters is not valid from the scope of a where access_type=virtual_wan_link_container.	No	Yes
wan_ingress_interactive_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified WAN link as their local WAN link will not be used for interactive traffic unless no other path is up. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Yes
wan_egress_interactive_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified WAN link as their remote WAN link will not be used for interactive traffic unless no other path is up. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Yes
wan_ingress_bulk_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified WAN link as their local WAN link will not be used for bulk traffic unless no other path is up. This parameters is not valid from the scope of a where access_type=virtual_wan_link_container.	No	Yes
wan_egress_bulk_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified WAN link as their remote WAN link will not be used for bulk traffic unless no other path is up. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Yes

Keyword	Type	Description	Required	Default
wan_ingress_trigger_dynamic_conduit_rate_kbps	Number	If the total ingress bandwidth used for this WAN link exceeds this rate, in kbps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Same as wan_ingress_permitted_rate_kbps
wan_egress_trigger_dynamic_conduit_rate_kbps	Number	If the total egress bandwidth used for this WAN link exceeds this rate, in kbps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	Same as wan_egress_permitted_rate_kbps
wan_ingress_trigger_dynamic_conduit_pps	Number	If the total ingress bandwidth used for this WAN link exceeds this rate, in pps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site. This parameters is not valid from the scope of a where access type=virtual wan link container.	No	-1 (In t2_app, 4294967295)
wan_egress_trigger_dynamic_conduit_pps	Number	If the total egress bandwidth used for this WAN link exceeds this rate, in pps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site. This parameters is not valid from the scope of a where access_type=virtual_wan_link_container.	No	-1 (In t2_app, 4294967295)
wan_ingress_permitted_rate_auto_learn	Boolean	Instead of specifying the ingress permitted rate for the specified link in the configuration, enabling this setting will cause the t2_app to automatically figure out this permitted rate. (Note: This does not mean that the user will get an error for setting the ingress permitted rate in the configuration)	No	No

Keyword	Type	Description	Required	Default
wan_egress_permitted_rate_auto_learn	Boolean	Instead of specifying the egress permitted rate for the specified link in the configuration, enabling this setting will cause the t2_app to automatically figure out this permitted rate. (Note: This does not mean that the user will get an error for setting the egress permitted rate in the configuration)	No	No
wan_link_mode	text	A WAN link can be configured in one of three modes: regular_active, last_resort_standby, on_demand_standby	No	regular_active
standby_wan_link_priority	number	If wan_link_mode is either last_resort_standby or on_demand_standby, the standby priority of the WAN link can be set to 1, 2, or 3. A priority value of 1 means the WAN link will be activated first.	No	1
standby_wan_link_heartbeat_interval_s	number	This parameter specifies the time interval at which 2 successive heartbeat control messages are sent when there is no other traffic on the path. The acceptable value is 010 seconds. If 0 is specified, no heartbeats are sent.	No	1
adaptive_bandwidth_detection	Boolean	Turn on passive bandwidth detection on this wan link	No	No
minimum_acceptable_bandwidth_for_abd_pct	Number	This percentage represents the minimum bandwidth level a usage can have before the passive bandwidth detection feature gives up and lets the paths on the usage go bad.	No	30
wan_link_template_name	Text	This field used by the config editor to load the values specified on the WAN Link template on to the WAN Link. Hand editing the config file will be ignored.	No	N/A

add service_group

Keyword	Type	Description	Required	Default
name	Text	Name of the service_group	Yes	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this service group	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this service group	Yes	N/A

Note: With the Talari APN provisioning process, we introduce the concept of Fair Shares. Shares are used to distribute the permitted bandwidth between the groups. The bandwidth calculated is based on the shares allocated for a particular group, divided by the total shares for all groups. A separate pool of shares is used for both Ingress and Egress traffic.

add net_usage

Keyword	Type	Description	Required	Default
service_type	Text	Type of service to be used on this link. When defined on a virtual_wan_link_container, this field is **limited to "intranet".**	Yes	N/A
intranet_service_name	Text	Name of intranet service to be used on this link.	Yes, if service_type=intranet	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage. This field is only valid from the scope of a non virtual wan link container.	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this usage. This field is only valid from the scope of a non virtual_wan_link_container.	Yes	N/A
use	Text	Declares if this WAN link the primary path for internet/intranet or a backup path that will only be used if the primary is no longer available or if the Talari will load balance across multiple internet links.	No	primary
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this WAN Link. If no group is specified, the default group is used. This field is only valid from the scope of a non virtual_wan_link_container.	No	**"Default"**
max_delay_ms	Number	Packets sent for this net usage that **take longer than "max_delay_ms" to** get to the WAN are dropped.	No	500
enable_wan_egress_grooming	Boolean	Determines whether WAN egress traffic should be groomed.	No	yes

Keyword	Type	Description	Required	Default
wan_ingress_dscp_tag_value	Text	Determines whether we should set the dscp tag of WAN ingress packets before sending them to the WAN, and what we should set it to. This field is only valid from the scope of a non virtual wan link container.	No	N/A
wan_egress_dscp_match_value	Text	Determines whether we should check the dscp tag of packets on WAN egress, and what value we should check against. This field is only valid from the scope of a non virtual_wan_link_container.	No	N/A
wan_egress_dscp_tag_value	Text	Determines whether we should set the dscp tag of WAN egress packets before sending them to the LAN, and what we should set it to.	No	N/A
tunnel hdr size bytes	Number	Size of the VPN tunnel header.	No	0
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	100
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	100
change_access_interface_upon_failure	Boolean	If set to yes, and onlky one access interface is defined in the WAN link, then a packet with VLAN/subnet other than the one defined in the access interface will be discarded.	No	Yes
wan_egress_maximum_allowed_bandwidth_kbps	Number	The maximumamount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	No limit
wan_ingress_maximum_allowed_bandwidth_kbps	Number	The maximumamount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	No limit

add dynamic_conduit_usage

Keyword	Type	Description	Required	Default
wan_ingress_rate_fair_share_for_all_dynamic_conduits	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage. This field is only valid from the scope of a non virtual wan link container.	Yes	N/A

Keyword	Type	Description	Required	Default
wan_egress_rate_fair_share_for_all_dynamic_conduits	Number	Number of shares for fair allocation of bandwidth on Egress for this usage. This field is only valid from the scope of a non virtual wan link container.	Yes	N/A
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this WAN Link. If no group is specified, the default group is used. This field is only valid from the scope of a non virtual_wan_link_container.	No	“Default”
tunnel_hdr_size_bytes	Number	Size of the VPN tunnel header.	No	0
enable_udp_hole_punching	Boolean	Enables the WAN link for use in udp hole punching	No	no
active_path_mtu_discovery_enable	Boolean	If enabled, the APNA will perform probes on all WAN Ingress paths for this service to determine the current MTU	No	no
udp_port_num	Number	This will be used as the source udp port for all wan ingress packets sent from this link. The APNA will also only accept wan egress packets at this link with dst_port set to this port number or the udp_pot_num_alt value if it is set.	No	2156
udp_port_num_alt	Number	This will be used as the alternate source udp port for all wan ingress packets sent from this link. The APNA will also only accept WAN egress packets at this link with dst_pot set to this port number or the udp_port_num value.	No	Defaults to udp_port_num
udp_port_switch_interval_minutes	Number	Interval in minutes to be used when switching between the 2 values of udp_port_num and udp_port_num_alt. Allowed values are from 1 minute to 8640 minutes (6 days).	No	1440 if udp_port_num and udp_port_num _alt are both set and are not equal
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	80

Keyword	Type	Description	Required	Default
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual wan link container.	No	80
wan_egress_maximum_allowed_bandwidth_kbps	Number	The maximumamount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	No limit
wan_ingress_maximum_allowed_bandwidth_kbps	Number	The maximumamount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual wan link container.	No	No limit
autopath_group_name	text	This field determines which autopath group this WAN Link Dynamic Conduit Usage belongs to. This implies that this link will only autogenerate paths to other WAN Links at other sites that are members of this same autopath group and are of the same access_type (public/private). If this field is not set and this is a public link, auto generated paths will be created between this link and other public links existing at other sites (the pre-autopath group behavior). If this field is not set and this is a private link, autogenerating paths is not permitted.	No	“”

add conduit_usage

Keyword	Type	Description	Required	Default
remote_site_name	Text	The remote site of the conduit that usage is being added for	Yes	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage. This field is only valid from the scope of a non virtual_wan_link_container.	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this usage. This field is only valid from the scope of a non virtual_wan_link_container.	Yes	N/A

Keyword	Type	Description	Required	Default
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this WAN Link. If no group is specified, the default group is used. This field is only valid from the scope of a non virtual_wan_link_container.	No	“Default”
tunnel_hdr_size_bytes	Number	Size of the VPN tunnel header.	No	0
enable_udp_hole_punching	Boolean	Enables the WAN link for use in udp_hole_punching	No	no
active_path_mtu_discovery_enable	Boolean	If enabled, the APNA will perform probes on all WAN Ingress paths for this service to determine the current MTU	No	no
udp_port_num	Number	This will be used as the source udp port for all wan ingress packets sent from this link. The APNA will also only accept wan egress packets at this link with dst_port set to this port number or the udp_pot_num_alt value if it is set.	No	2156
udp_port_num_alt	Number	This will be used as the alternate source udp port for all wan ingress packets sent from this link. The APNA will also only accept WAN egress packets at this link with dst_pot set to this port number or the udp_port_num value.	No	Defaults to udp_port_num
udp_port_switch_interval_minutes	Number	Interval in minutes to be used when switching between the 2 values of udp_port_num and udp_port_num_alt. Allowed values are from 1 minute to 8640 minutes (6 days).	No	1440 if udp_port_num and udp_port_num _alt are both set and are not equal
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual wan link container.	No	80
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	80

Keyword	Type	Description	Required	Default
wan_egress_maximum_allowed_bandwidth_kbps	Number	The maximum amount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual wan link container.	No	No limit
wan_ingress_maximum_allowed_bandwidth_kbps	Number	The maximum amount of WAN egress bandwidth that this usage will be allowed in scheduling. This field is only valid from the scope of a non virtual_wan_link_container.	No	No limit
autopath_group_name	text	This field determines which autopath group this WAN Link Conduit Usage belongs to. This implies that this link will only autogenerate paths to other WAN Links at other sites that are members of this same autopath group and are of the same access_type (public/private). If this field is not set and this is a public link, auto generated paths will be created between this link and other public links existing at other sites (the pre-autopath group behavior). If this field is not set and this is a private link, autogenerating paths is not permitted.	No	“”

add cos_wan_link

set properties

Keyword	Type	Description	Required	Default
ip_dscp	Text	The DSCP tag for the MPLS Queue described by this object	No	“default”
use_for_unmatched_tag	Boolean	If enabled, DCSP tags not matched by other MPLS Classes will use this Class. One, and only one, MPLS Class must be marked for use by unmatched tags.	No	No
wan_ingress_perm itted_rate_kbps	Number	Available rate of the MPLS Queue for WAN ingress traffic	Yes	N/A
wan_egress_permitted_rate_kbps	Number	Available rate of the MPLS Queue for WAN Egress traffic	Yes	N/A
tracking_ip_addr	IP Address	The virtual IP that will be correlated with the state of this MPLS Queue, allowing it be tracked via ping.	No	N/A
congestion_threshold_us_per_s_us	Number	The number of microseconds per second of congestion that must be detected on a MPLS Queue before it goes into congestion avoidance mode.	No	20000
wan_ingress_realtime_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified MPLS Queue as their local WAN link will not be used for realtime traffic unless no other path is up.	No	Yes
wan_egress_realtime_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified MPLS Queue as their remote WAN link will not be used for realtime traffic unless no other path is up.	No	Yes

Keyword	Type	Description	Required	Default
wan_ingress_interactive_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified MPLS Queue as their local WAN link will not be used for interactive traffic unless no other path is up.	No	Yes
wan_egress_interactive_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified MPLS Queue as their remote WAN link will not be used for interactive traffic unless no other path is up.	No	Yes
wan_ingress_bulk_eligible	Boolean	If set to “no”, WAN ingress paths at the local site with the specified MPLS Queue as their local WAN link will not be used for bulk traffic unless no other path is up.	No	Yes
wan_egress_bulk_eligible	Boolean	If set to “no”, WAN ingress paths at other sites with the specified MPLS Queue as their remote WAN link will not be used for bulk traffic unless no other path is up.	No	Yes
wan_ingress_trigger_dynamic_conduit_rate_kbps	Number	If the total ingress bandwidth used for this MPLS Queue exceeds this rate, in kbps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site.	No	Same as wan_ingress_permitted_rate_kbps
wan_egress_trigger_dynamic_conduit_rate_kbps	Number	If the total egress bandwidth used for this MPLS Queue exceeds this rate, in kbps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site.	No	Same as wan_egress_permitted_rate_kbps
wan_ingress_trigger_dynamic_conduit_pps	Number	If the total ingress bandwidth used for this MPLS Queue exceeds this rate, in pps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site.	No	-1 (Int2_app, 4294967295)
wan_egress_trigger_dynamic_conduit_pps	Number	If the total egress bandwidth used for this MPLS Queue exceeds this rate, in pps, at an intermediate site, the intermediate site will signal the dynamic conduit creating sites to create dynamic conduits, instead of sending multihop traffic through the intermediate site.	No	-1 (Int2_app, 4294967295)

add service_group

Keyword	Type	Description	Required	Default
Name	Text	Name of the service group.	Yes	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this service_group	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this service_group	Yes	N/A

add conduit_usage

Keyword	Type	Description	Required	Default
remote_site_name	Text	The remote site of the conduit that usage is being added for	Yes	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this usage	Yes	N/A
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this MPLS Queue. If no group is specified, the default group is used.	No	“Default”
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling.	No	80
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling.	No	80
wan_egress_maximum_allowed_bandwidth_kbps	Number	The maximum amount of WAN egress bandwidth that this usage will be allowed in scheduling.	No	No limit
wan_ingress_maximum_allowed_bandwidth_kbps	Number	The maximum amount of WAN egress bandwidth that this usage will be allowed in scheduling.	No	No limit
autopath_group_name	Text	This field determines which autopath group this MPLS Queue Conduit Usage belongs to. This implies that this link will only autogenerate paths to other MPLS Queues at other sites that are members of this same autopath group. Setting this value to “Inherit” will cause this value to be set to the corresponding value on this conduit_usage for the parent virtual_wan_link_container object.	No	“”

add dynamic_conduit_usage

Keyword	Type	Description	Required	Default
wan_ingress_rate_fair_share_for_all_dynamic_conduits	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage	Yes	N/A
wan_egress_rate_fair_share_for_all_dynamic_conduits	Number	Number of shares for fair allocation of bandwidth on Egress for this usage	Yes	N/A
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this MPLS Queue. If no group is specified, the default group is used.	No	"Default"
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling.	No	80
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling.	No	80
wan_egress_maximum_allowed_bandwidth_kbps	Number	The maximum amount of WAN egress bandwidth that this usage will be allowed in scheduling.	No	No limit

add net_usage

Keyword	Type	Description	Required	Default
service_type	Text	Type of service to be used on this link. From the scope of an MPLS Queue, this **must always be "intranet"**	Yes	N/A
intranet_service_name	Text	Name of intranet service to be used on this link	Yes, if service_type=intranet	N/A
wan_ingress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Ingress for this usage	Yes	N/A
wan_egress_rate_fair_share	Number	Number of shares for fair allocation of bandwidth on Egress for this usage	Yes	N/A

Keyword	Type	Description	Required	Default
service_group_name	Text	Name of the service group that this usage will belong in. The bandwidth allocated to this usage comes out of the fair_share allocated to the group associated with this name for this WAN Link. If no group is specified, the default group is used.	No	“Default”
max_delay_ms	Number	Packets sent for this net usage that take longer than “max_delay_ms” to get to the WAN are dropped.	No	500
enable_wan_egress_grooming	Boolean	Determines whether WAN egress traffic should be groomed.	No	yes
wan_egress_dscp_tag_value	Text	Determines whether we should set the dscp tag of WAN egress packets before sending them to the LAN, and what we should set it to. Setting this value to “Inherit” will cause this value to be set to the corresponding value on this intranet usage for the parent virtual_wan_link_container object.	No	N/A
wan_egress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN egress bandwidth that this usage will be reduced to during on-demand scheduling.	No	100
wan_ingress_minimum_reserved_bandwidth_kbps	Number	The minimum amount of WAN ingress bandwidth that this usage will be reduced to during on-demand scheduling.	No	100

add ha_appliance

Keyword	Type	Description	Required	Default
name	Text	The name to be used when referencing this appliance through the configuration and user interfaces.	Yes	N/A

add ha_service

set properties

Keyword	Type	Description	Required	Default
primary_appliance_name	Text	Name of the appliance to be used as the primary appliance if primary_reclaim=yes, otherwise just the name of either appliance.	Yes	N/A
secondary_appliance_name	Text	Name of the appliance to be used as the secondary appliance if primary_reclaim=yes, otherwise just the name of either appliance.	Yes	N/A
failover_ms	Number	How long the standby HA appliance should wait to take over active state after losing contact with active appliance.	No	1000
primary_reclaim	Boolean	Whether the primary HA appliance should forcefully take back the active role from the secondary	No	no
shared_mac	MAC Address	Base MAC address for the HA appliances to use	No	AA:AA:AA:00:00:00
use_serial_ha	Boolean	Specifies whether or not HA and fail-to-wire will be allowed.	No	no

Note:
1. When deploying high-availability appliances in a fully-inline topology, Spanning Tree Protocol (STP) is used to prevent network loops. As a result, when one of the appliances in a pair goes down, STP will block communication between them for up to 40 seconds. Because of this communication loss, the primary appliance will ALWAYS reclaim in this scenario regardless of the configuration setting.

2. When using high-availability appliances in one-arm mode, if the only link on the primary appliance goes down, both primary and secondary appliances will become active. When the port on the primary box comes up again, the primary appliance will stay active and the secondary appliance switches to standby - no matter what the primary reclaim setting is.

set interface_properties

Keyword	Type	Description	Required	Default
virtual_interface_name	Text	A virtual interface that the HA appliances will use to communicate. All other parameters defined in the interface group are in reference to this virtual interface	Yes	N/A

Keyword	Type	Description	Required	Default
primary_ip_addr	IP Address	Unique virtual IP address that the primary appliance will use to communicate with its peer	Yes	N/A
secondary_ip_addr	IP Address	Unique virtual IP address that the secondary appliance will use to communicate with its peer	Yes	N/A

add external_tracker

Keyword	Type	Description	Required	Default
ip_addr	IP Address	The virtual IP that will be correlated with the state of this device. This IP references and external device that responds to ARP requests that is reachable from the virtual interface specified in the containing scope.	Yes	N/A

Define WAN-to-WAN Forwarding Group

Syntax

Note: All parameters listed in square brackets [] are optional.

```
[define wan_to_wan_forwarding_group name=text ]
{

}
```

Commands and Parameters

set apn_properties

Keyword	Type	Description	Required	Default
encryption_mode	Text	Sets the encryption schema for all conduit encryption in the defined network. Acceptable values are **“aes128” and “aes256”.**	no	aes128
encryption_rekey_enabled	boolean	In enabled, Encryption Keys are rotated at intervals of 10-15 minutes	no	yes
enhanced_message_authentication	boolean	If enabled, a 4 byte trailer is appended to the contents of encrypted traffic to verify the contents is delivered unaltered	no	No
enhanced_message_authentication_type	Text	Sets the type of authentication code to use for enhanced_message_authentication. Ac**ceptable values are “checksum” and “sha256”**	No	checksum
enhanced_packet_uniqueness	boolean	If enabled, a 16 byte encrypted counter is prepended to encrypted traffic to serve as an Initialization Vector and randomize packet encryption	no	no
firewall_default_action	Text	The action for packets the do not match a policy. This policy may be overridden at an Appliance.	no	"allow"
firewall_policy_template_name	Text	A Firewall Policy template to be applied to all Appliances in the APN.	no	N/A
default_track_connection	Boolean	Enables or disables Connection state tracking for packets not matching a filter policy. This setting may be overridden at an Appliance.	No	No

Keyword	Type	Description	Required	Default
compiler_version	Text	Used exclusively by the compiler. For example to use in migration of Conduit Service Class for auto adjusting Interactive and Bulk Classes during migration one time and not after that.	No	7_0

define firewall_zone

Keyword	Type	Description	Required	Default
name	Text	The name of the zone to be referenced in the configuration	Yes	N/A

define firewall_policy_template

Keyword	Type	Description	Required	Default
name	Text	The name of the firewall_policy_template, whose rules we are defining. This name will **be specified on the Site's firewall, where** these rules are to be applied.	Yes	N/A

add pre_appliance_policies

This bracket separated section will contain all of the policies that will be applied for this template BEFORE the policies defined explicitly on the firewall. Please see the "add firewall filter" section for more detail on firewall filters.

add post_appliance_policies

This bracket separated section will contain all of the policies that will be applied for this template AFTER the policies defined explicitly on the firewall. Please see the "add firewall filter" section for more detail on firewall filters.

Define Application

Syntax

Note: All parameters listed in square brackets [] are optional.

```
[define application name=text]
{
        set application_properties
                [gather_mos={true|false}];
}
```

Commands and Parameters

set application_properties

Keyword	Type	Description	Required	Default
name	Text	The name of the application whose properties we are defining. The name used by rule -, properties -, application_name is a reference to this name. Rules whose application_name are equal to this Text will be aggregated together for statistical purposes on a per site, per conduit basis.	Yes	N/A
gather_mos	Boolean	If enabled, statistics pertinent to MOS estimation will be collected for each rule that references this application. MOS will be calculated for each conduit over all rules for this application at that conduit.	No	No

Define Routing Domain

Syntax

Note: All parameters listed in square brackets [] are optional.

```
[define routing_domain name=text]
{
        set routing_domain_properties
                [is_default={yes|no}] ;
}
```

Commands and Parameters

Keyword	Type	Description	Required	Default
Name	Text	This is the name of the Routing Domain When configuring routing domains for VRF functionality, using this routing domain for the appropriate objects will denote that those objects are only usable for that Routing Domain (for more information on VRF, see vrf_design.odt	Yes	N/A

set routing_domain_properties

Keyword	Type	Description	Required	Default
is_default	Boolean	This is the routing_domain to be used when the user has implicitly/explicitly denoted that they wish to use the default routing_domain option.	No	No

Define Net_Object

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define net_object name=text { }
{
        add network
                ip_addrn=x.x.x.x/n
        ;
}
```

Commands and Parameters

Keyword	Type	Description	Required	Default
Name	Text	This is the name of the network object.	Yes	N/A

add network

Keyword	Type	Description	Required	Default
ip_addrn	Network Address	This is an IP address and netmask/prefix used to define the network for this network object.	No	No

Define dhcp_option_set

Commands and Parameters

Keyword	Type	Description	Required	Default
name	Text	The name of the dhcp option set that will be used to reference this set in a given dhcp subnet **range in order to include the set's options within** that range object.	Yes	N/A

add dhcp_option

Keyword	Type	Description	Required	Default
is_option	Boolean	Set to true for options and false for parameters	No	Yes
option_name	Text	vendor_encapsulated_options|netbios_name_servers|netbios_node_type|tftp_server_name|tftp_server_address|ip_telephone|custom|max_lease_time | default_lease_time | subnet_mask | routers | domain_name_servers |domain_name	Yes	N/A
option_number	Number	1| 3| 6| 15|43 | 44 | 46 | 66 | 150 | 176 | 224 - 254. Auto set. Required only for option_name=custom. (subnet=1, routers=3, domain_name_servers=6, domain_name=15,vendor_encapsulated_options = 43, netbios_name_servers=44, netbios_node_type=46, tftp_server_name=66, tftp_server_address=150, ip_telephone=176,custom=224-254, other all are 0 or basically doesnt matter)	Yes	N/A
value	Number, IP Address or Text	depends on the data_type. But this is the value for the corresponding option number.	Yes	N/A
data_type	Text	string|domain_name|ip_address||integer .Auto set. Required only for option_name=custom. Required only for option_name=custom. (vendor_encapsulated_options= string, netbios_name_servers=ip_address, netbios_node_type=integer, tftp_server_name=integer,tftp_server_address=string, ip_telephone=string, max_lease_time=integer, default_lease_time=integer,subnet_mask=ip_address,domain_name_servers=ip_address, domain_name=domain_name	Yes	N/A

Define Application Match Collection

Note: Defining multiple collection objects will simply map all of the application_match objects into a single application_match_collection object, populated in the same order each application was encountered on parse.

define application_match_collection

Keyword	Type	Description	Required	Default
Name	Text	This is the name of the Application Match Object. This name will be used to reference this application match by rules and firewall filters.	Yes	N/A

set application_match_properties

Keyword	Type	Description	Required	Default
enabled	Boolean	A disabled application_match cannot be used by any filter or rule, and will not be included in the registry for statistics collection in the t2_app.	No	No
application_category	Text	Application category the application belongs to.	No	Other
application_classification	Text	How the traffic of the application will be handled for QoS. Valid options are: bulk_p1, bulk_p2, interactive_p1, interactive_p2, interactive_p3, interactive_p4, real_time_p1, real_time_p2.	No	bulk_p1
probing_interval_s	Number	Application probing interval in seconds. Valid options are: 0, 10, 60, 120, 300.	No	0
response_time_normal_ms	Number	For application probing, the normal round trip time in mS. Valid range: 2 - 2000	No	100
response_time_warning_ms	Number	For application probing, the warning round trip time in mS. Valid range: 2 - 2000		200

add application_match_criteria

Keyword	Type	Description	Required	Default
ip_addrn1	IP Addr / Prefix	The network IP address space for either the source or destination IP of a packet to match in order to still match this application. If both ip_addrn1 and ip_addrn2 are set, then the packet's source and destination must match each of the source and destination IPs of the packet. (ie - (ip_addrn1=src and ip_addrn2=dst) OR (ip_addrn1=dst and ip_addrn2=src))	No	N/A

Keyword	Type	Description	Required	Default
ip_addrn2	IP Addr/ Prefix	The network IP address space for either the source or destination IP of a packet to match in order to still match this application. If both ip_addrn1 and ip_addrn2 are set, then the packet's source and destination must match each of the source and destination IPs of the packet. (ie - (ip_addrn1=src and ip_addrn2=dst) OR (ip_addrn1=dst and ip_addrn2=src))	No	N/A
port_num1	Number	The port for either the source or destination port of a packet to match in order to still match this application. If both port_num1 and port_num2 are set, then the packet's source and destination must match each of the source and destination ports of the packet. (ie - (port_num1=src and port_num2=dst) OR (port_num1=dst and port_num2=src))	No	N/A
port_num2	Number	The port for either the source or destination port of a packet to match in order to still match this application. If both port_num1 and port_num2 are set, then the packet's source and destination must match each of the source and destination ports of the packet. (ie - (port_num1=src and port_num2=dst) OR (port_num1=dst and port_num2=src))	No	N/A
domain_name	Text	Valid domain name like www.facebook.com, “facebook”, “outlook365”.	No	N/A
ip_protocol_num	Number	The protocol number of a packet to match in order to still match this application.	No	N/A
ip_dscp	Text	The DSCP tag of a packet to match in order to still match this application.	No	N/A

Define application_category

Parameters

Keyword	Type	Description	Required	Default
Name	String	The name of this application category.	Yes	N/A

set application_category_properties

Keyword	Type	Description	Required	Default
talari_defined	Boolean	This should only be set true for Talari defined application categories.	No	False

Define site_group_object

Parameters

Keyword	Type	Description	Required	Default
Name	String	The name of this site group	Yes	N/A

add application_site

Keyword	Type	Description	Required	Default
Name	String	The name of site to be added to the site group.	Yes	N/A

Add application_policy

Parameters

Keyword	Type	Description	Required	Default
Name	String	The name of this application policy.	Yes	N/A

Set application_policy_properties

Keyword	Type	Description	Required	Default
enabled	Boolean	A disabled application_policy will not be included in the registry for t2_app.	No	Yes
routing_domain	Text	The routing domain name this policy will be applied to.	No	Default routing domain of the APN.
destination_site	Text	All traffic for the matching applications will use **this site's specified service. Valid options are:** local or a valid site name in APN.	No	Default to local

Keyword	Type	Description	Required	Default
destination_service_type	Text	The service will be used when direct matching applications to the destination site. Valid options are: Default (use normal destination based routing), internet, intranet.	Yes	
destination_service	Text	The name of the service if Intranet		
classification	Text	The QoS for the matching applications. Valid **options are: "", bulk_p1, bulk_p2, interactive_p1,** interactive_p2, interactive_p3, interactive_p4, real_time_p1, real_time_p2.	No	Use application classification.

define service_provider

Keyword	Type	Description	Required	Default
Name	String	The name of this service provider in which the underlying wan_link_template_objects are specified.	Yes	N/A

add wan_link_template

Keyword	Type	Description	Required	Default
Name	String	The name of this template, as referecened by the virtual_wan_links that implement its settings.	Yes	N/A

set wan_link_template_properties

Keyword	Type	Description	Required	Default
link_type		Can only be set to MPLS, broadband, or private_link. WAN Link Templates with a link type of MPLS can only be applied to cos_wan_link_container. broadband and private_link types can only be applied to virtual_wan_link.	No	broadband

Keyword	Type	Description	Required	Default
wan_ingress_physical_rate_kbps	Integer	This is the value that the WAN Link will use for its wan_ingress_physical_rate_kbps setting, upon applying this template.	Yes (no audit for this directly, it will apply zero to all of your links, and those links will be invalid)	N/A
wan_egress_physical_rate_kbps	Integer	This is the value that the WAN Link will use for its wan_egress_physical_rate_kbps setting, upon applying this template.	Yes (no audit for this directly, it will apply zero to all of your links, and those links will be invalid)	N/A
wan_ingress_permitted_rate_auto_learn	Boolean	This is the value that the WAN Link will use for its wan_ingress_permitted_rate_auto_learn setting, upon applying this template. **Note**: If this value is not enabled, then the permitted rate for the link where this template is applied will be set to the physical rate in this same direction.	No	Yes (Although the basic editor will default this value to No upon creation from the basic sites)

Keyword	Type	Description	Required	Default
wan_egress_permitted_rate_auto_learn	Boolean	This is the value that the WAN Link will use for its wan_egress_permitted_rate_auto_learn setting, upon applying this template. **Note**: If this value is not enabled, then the permitted rate for the link where this template is applied will be set to the physical rate in this same direction.	No	Yes (Although the basic editor will default this value to No upon creation from the basic sites)
autopath_group_name	String	This is the name of the autopath_group we will apply to all of the conduit and dynamic conduit usages on the WAN Link. **Note**: No errors will be displayed to the user if conduit/dynamic conduit usages under the link have autopath groups explicitly defined. The compiler will just silently overwrite these values. **Additional Note:** In the instance that a link_type **of "mpls" is selected and no autopath group is** explicitly set for this template, a new defaulted autopath group will be created in the **configuration names "<service provider name>_mpls", and that** autopath group name will be set here.	No	""

add wan_link_template_mpls_queue

Note: If this template is applied to an existing MPLS link, all pre-existing queues on that link will be removed and replaced with defaulted queues auto-generated wit the below settings changed.

Parameters

Keyword	Type	Description	Required	Default
ip_dscp	Text	This is the ip_dscp setting that will be used in the auto-generated MPLS queue on the link where this template will be applied.	No	**"default"**

Keyword	Type	Description	Required	Default
wan_ingress_permitted_rate_kbps	Integer	This is the wan_ingress_permitted_rate_kbps setting that will be used in the auto-generated MPLS queue on the link where this template will be applied	Yes	N/A
wan_egress_permitted_rate_kbps	Integer	This is the wan_egress_permitted_rate_kbps setting that will be used in the auto-generated MPLS queue ion the link where this template will be applied.	Yes	N/A

Define Autopath Group

Syntax

Note: All parameters listed in square brackets [] are optional.

```
[define autopath_group name=text]
{
        set autopath_group_properties
                [enable_encryption={yes|no}]
                [enable_instability_sensitivity={yes|no}]
                [enable_bad_loss_sensitivity={yes|no}]
                [is_default={yes|no}]
        [path_loss_threshold_pct=1..90]
                [path_loss_threshold_over_time_ms=100..2000]
                [silence_sensitivity_period_ms=150..1000]
                [path_bad_to_good_probation_period_ms=500..60000]
                [is_default={yes|no}]
        [ip_dscp={af11|af12|af13|af21|af22|af23|af31|af32|af33|af41|af42|af43|cs1|cs2|
cs3|cs4|cs5|cs6|cs7|default|ef};
}
```

Commands and Parameters

Keyword	Type	Description	Required	Default
Name	Text	The name of the autopath group.	Yes	N/A

set autopath_group_properties

Keyword	Type	Description	Required	Default
enable_encryption	Boolean	For paths automatically generated in this autopath group, this will be the value of the **generated path's "enable encryption" parameter.**	No	Yes

Keyword	Type	Description	Required	Default
enable_instability_sensitivity	Boolean	For paths automatically generated in this autopath group, this will be the value of the generated path's “enable_instability_sensitivity” parameter.	No	Yes
enable_bad_loss_sensitivity	Boolean	For paths automatically generated in this autopath group, this will be the value of the generated path's “enable_bad_loss_sensitivity” parameter.	No	Yes
path_loss_threshold_pct	Number	Percentage threshold before path is considered bad. This threshold is measured over specified time. When this field is not specified, the default is to measure packet loss based on the last received 200 packets. Valid value are 1-90%	No	N/A
path_loss_threshold_over_time_ms	Number	Specify sample period over which to evaluate packet loss. Used in conjunction with path_loss_threshold_pct. Valid values are 100-2000ms	No	1000
silence_sensitivity_period_ms	Number	Specify silence duration before Path state transitions from GOOD to BAD. Valid values are 150-1000ms	No	150ms
path_bad_to_good_probation_period ms is set	Number	Specify the probation period to wait before moving Path state transitions from BAD to GOOD. Valid values are 500-60000ms	No	10000
ip_dscp	Text	For paths automatically generated in this autopath group, this will be the value of the generated path's “ip_dscp” parameter.	No	N/A
is_default	Boolean	This denotes that an autopath_group is the “default” autopath group. When an autopath_group_name on the conduit/dynamic conduit usage references the string “Default”, this will correspond with whichever autopath group has the is_default flag enabled. No more, and no less. There must be one and only one autopath group in the configuration can have this flag turned on. In the event of a pre 3.0 configuration migration, an autopath_group will be automatically generated with this flag enabled.	No	No

Dynamic Conduit Default Set

This object allows the user to define a dynamic conduit’s rule defaults.

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define dynamic_conduit_default_set name=text
{
        set ipsec_properties
                enabled = [yes|no]
                tunnel mode = [esp|esp auth|ah]
```

```
            encryption_mode = [aes128|aes256]
            hash_algorithm = [sha|sha256];
            lifetime_s = [0...86400];
      [set realtime_class]
            class_id=n
            [initial_rate_pct=p]
            sustained_rate_pct=p
            [initial_period_ms=n] ;

      [set interactive_class]
            class_id=n
            [initial_share_pct=p]
            sustained_share_pct=p
            [initial_period_ms=n] ;

      [set bulk_class]
            class_id=n
            [bulk_share_pct=p]
            [delay_min_depth_bytes=n];

      [set dynamic_conduit_properties]
            [create_conduit_sampling_time_seconds=n]
            [create_conduit_wan_ingress_min_throughput_rate_kbps=n]
            [create_conduit_wan_egress_min_throughput_rate_kbps=n]
            [create_conduit_wan_ingress_min_pps=n]
            [create_conduit_wan_egress_min_pps=n]
            [remove_conduit_sampling_time_minutes=n]
            [remove_conduit_wan_ingress_througput_rate_kbps=n]
            [remove_conduit_wan_egress_througput_rate_kbps=n]
            [remove_conduit_wan_ingress_pps=n]
            [remove_conduit_wan_egress_pps=n]
            [remove_conduit_down_wait_time_minutes=n]
            [recreate_conduit_hold_time_minutes=n]

      [add rule]
      {
            [set properties]
                  [precedence={high | medium | low}]
                  [application_name=text]
                     [track_performance={yes | no}]

            set match_criteria
                  [ip_addrn=x.x.x.x/n]
                  [src_ip_addrn=x.x.x.x/n]
                  [dst_ip_addrn=x.x.x.x/n]
                  [port_num=n-n]
                  [src_port=n-n]
                  [dst_port=n-n]
                  [ip_protocol_num=n]
                  [ip_dscp=aaxx]
```

```
                    [ip_tos_match_flows={yes | no}]
                    [rouing_domain=text]
                    [vlan_id={native | 0...4094}]
                    [protocol_str={ * | FTP | SMTP | HTTP | TELNET | ICMP |
HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

          [set traffic_optimization_properties]
                    [enable_tcp_termination={yes | no}]
                    [enable_packet_aggregation={yes | no}];

          [set ingress_properties]
                    [class_id=n]
                    [class_name=text]
                    [class_tail_drop_small_packet_ms=n]
                    [class_tail_drop_small_packet_bytes=n]
                    [class_tail_drop_large_packet_size_bytes=n]
                    [class_tail_drop_packet_ms=n]
                    [class_tail_drop_packet_bytes=n]
                    [class_dup_disable_depth_greater_ms=n]
                    [class_dup_disable_depth_greater_bytes=n]
                    [reassign_flow_if_packet_exceeds_size_bytes=n]
                    [reassign_flow_if_packet_exceeds_size_class_id=n]
                    [reassign_flow_if_packet_exceeds_size_class_name=text]

     [reassign_class_tail_drop_small_packet_ms=n]
                    [reassign_class_tail_drop_small_packet_bytes=n]
                    [reassign_class_tail_drop_large_packet_size_bytes=n]
                    [reassign_class_tail_drop_packet_ms=n]
                    [reassign_class_tail_drop_packet_bytes=n]
                    [reassign_class_dup_disable_depth_greater_ms=n]
                    [reassign_class_dup_disable_depth_greater_bytes=n]
                    [tcp_standalone_ack_class_id=n]
                    [tcp_standalone_ack_class_name=text]

        [tcp_standalone_ack_class_tail_drop_small_packet_ms=n]
                    [tcp_standalone_ack_class_tail_drop_small_packet_bytes=n]

     [tcp_standalone_ack_class_tail_drop_large_packet_size_bytes=n]
                    [tcp_standalone_ack_class_tail_drop_packet_ms=n]
                    [tcp_standalone_ack_class_tail_drop_packet_bytes=n];

          set wan_properties
                    [transmit_mode={load_balance_paths | duplicate_paths |
persistent_path}]
                    [retransmit_lost_packets={yes | no}];

          set egress_properties
                    [resequence_packets={yes | no}]
                    [resequence_holdtime_ms=n]
                    [discard late resequence packets={yes | no}]
```

```
                    [dscp_tag_value=aaxx];

                [set deep_packet_inspection_properties]
                    [enable_passive_ftp_detection={yes | no}] ;
            }
        }
```

Commands and Parameters

Keyword	Type	Description	Required	Default
name	Text	The name to be used when referencing this default set through the configuration and user interfaces.	Yes	N/A

set advanced_properties

Keyword	Type	Description	Required	Default
activate_standby_bandwidth_threshold_percentage	number	This is the percentage of the total fair share rates of the associated WAN links in a conduit. When the available bandwidth provided by the regular active WAN links in a conduit drops below this threshold, on-demand standby WAN links are activated to supplement bandwidth.	Yes, but only when on-demand standby wan links are configured	N/A

Note: A dynamic_conduit_default_set contains all of the same parameters as a conduit_default_set, but with the following differences:

1. Classes have no initial/sustained kbps parameters.
2. The dynamic_conduit_default_set contains its own set of properties, **as described below**.

set dynamic_conduit_properties

Keyword	Type	Description	Required	Default
create_conduit_sampling_time_seconds	Number	This is the amount of time over which packet counts/bandwidth will be measured in order to determine if a dynamic conduit needs to be created between two sites.	No	1

Keyword	Type	Description	Required	Default
create_conduit_min_throughput_rate_kbps	Number	Within the time frame specified by create_conduit_sampling_time_seconds, if the total bandwidth in either direction between two sites where a dynamic conduit can be created exceeds this throughput measured in kbps, then a dynamic conduit will be created between those two sites.	No	200
create_conduit_min_pps	Number	Within the time frame specified by create_conduit_sampling_time_seconds, if the total bandwidth in either direction between two sites where a dynamic conduit can be created exceeds this throughput measured in pps, then a dynamic conduit will be created between those two sites.	No	10
remove_conduit_sampling_time_minutes	Number	This is the amount of time over which packet counts/bandwidth will be measured in order to determine if a dynamic conduit needs to be removed between two sites.	No	10
remove_conduit_througput_rate_kbps	Number	Within the time frame specified by remove_conduit_sampling_time_minutes, if the throughput of a dynamic conduit between two sites drops below this throughput in kbps, then the dynamic conduit between these two sites will be removed.	No	50
remove_conduit_pps	Number	Within the time frame specified by remove_conduit_sampling_time_minutes, if the throughput of a dynamic conduit between two sites drops below this throughput in pps, then the dynamic conduit between these two sites will be removed.	No	1
remove_conduit_down_wait_time minutes	Number	If a dynamic conduit goes dead for longer than this time frame, the dynamic conduit between these two sites will be removed.	No	5
recreate_conduit_hold_time_minutes	Number	If a dynamic conduit is removed because the dynamic conduit has been dead for too long, then a dynamic conduit between these two sites cannot be created again until this time frame elapses.	No	10

set realtime_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<class_id>
initial_rate_pct	Percent	Defines the maximum initial rate in as a percentage of the conduit total bandwidth that this class may consume while the queue depth is less than initial_period_ms.	No	initial_rate_kbps
sustained_rate_pct	Percent	Defines the rate this class will use of the conduit bandwidth as a percent share of the entire conduit.	No	sustained_rate_kbps
initial_period_ms	Number	Defines the queue depth at which switch is made between initial_rate and sustained rate.	No	0

set interactive_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<classid>
initial_share_pct	Percent	Defines the maximum initial rate in as a percentage of the conduit total bandwidth that this class may consume while the queue depth is less than initial_period_ms.	No	sustained_share_pct
sustained_share_pct	Percent	Defines the rate this class will use of the conduit bandwidth as a percent share of the entire conduit.	Yes	N/A
initial_period_ms	Number	Defines the queue depth at which switch is made between initial_rate and sustained_rate.	No	0

set bulk_class

Keyword	Type	Description	Required	Default
class_id	Number	A number from 0-9 that represents this class's index.	Yes	N/A
class_name	Text	A text name that can be used to reference this class.	No	class_<classid>
bulk_share_pct	Percent	Percentage of the all the bulk classes' share of the conduit bandwidth that this class will use.	No	1

add rule

set properties

Keyword	Type	Description	Required	Default
precedence	Text	Provides up to three sets of rules that will be scanned in priority order. First match found is taken. Order of rules is priority and then listed order in the config. All high priorities will be scanned, in the order listed, then mediums and then lows. There is no best match, only first match; so for example, more generalized IP networks (/32) should be placed in the low priority and last in order in order to allow more specific matches to take.	No	low
application_name	Text	A name given to a rule that will allow rule statistics to be summed in groups when they are displayed. All rule statistics for rules with the same application_name can be viewed together.	No	N/A
track_performance	Boolean	If yes, performance of a rule over time will be recorded in a session DB including loss, latency, jitter and bandwidth used.	No	no

set match_criteria

Keyword	Type	Description	Required	Default
ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed. If either source or destination matches this, then rule is hit.	No	N/A
src_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
dst_ip_addrn	Network Address	If defined, an IP subnet. If no subnet defined, /32 is assumed.	No	N/A
port_num	Range	If set, if either the destination or source port matches this number, the packet will hit the rule.	No	N/A
src_port	Range	If set, if the source port matches this number, the packet will hit the rule.	No	N/A
dst_port	Range	If set, if the destination port matches this number, the packet will hit the rule.	No	N/A
ip_protocol_num	Number	Defines an explicit protocol number as is set in the packets IP protocol field in the IP header.	No	N/A
ip_dscp	Text	Defines an explicit DSCP tag as is set in IP protocol fields in the IP header.	No	N/A

Keyword	Type	Description	Required	Default
ip_tos_match_flows	Boolean	If set to YES, ip_tos will be included as a criterion for creating new flows.	No	No
protocol_str	Text	Defines protocol that the filter will match. In particular, this rule represents the protocol type bits in the TCP header or the IP header as well as common ports for this protocol.	No	N/A
routing_domain	Text	This is the routing domain that this rule will match. If the user sets this to a specific domain, only traffic on that domain will be eligible to match this rule. If the user chooses not to set this value, ALL domains are eligible to match this domain.	No	N/A
vlan_id	Number	This is the VLAN ID that this rule will match. If the user sets this parameter to number (0-4096) only traffic tagged with that VLAN ID will be considered eligible to match this rule. Otherwise, if the user does not set this value, ALL VLAN IDs are eligible to match this rule.	No	N/A
application_match_name	Text	The application_match object that a packet must match for this rule. Note: If this field is set, IP address, port, protocol and dscp match settings for this rule will not be used in matching this rule.	No	N/A

set traffic_optimization_properties

Keyword	Type	Description	Required	Default
enable_tcp_termination	Number	This parameter is used to enable or disable the TCP Termination feature on this (TCP-based) rule.	No	No
enable_wan_op	Boolean	This parameter is used to enable or disable the WAN Optimization feature on this (TCP-based) rule.	No	No
other_header_compression_enabled	Boolean	If true, the we will perform header compression. If false, we should not. Applicable to IP, UDP, TCP headers.	No	No
gre_header_compression_enabled	Boolean	If true, we should perform GRE header compression. If false, we should not. Only supported when protocol is GRE or 47.	No	Yes for GRE, no for any other
enable_packet_aggregation	Boolean	If true, we should aggregate conduit user packet data packets that match this rule. If false, we should not aggregate packets that match this rule	No	no

Keyword	Type	Description	Required	Default
enable_tcp_termination	Number	This parameter is used to enable or disable the TCP Termination feature on this (TCP-based) rule.	No	No

set ingress_properties

Keyword	Type	Description	Required	Default
class_id	Number	Defines the class number that is to service traffic flows that match this rule.	One and only one of these two parameters must be set.	N/A
class_name	Text	Defines the class name that is to service traffic flows that match this rule.		N/A
class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than "class_tail_drop_large_packet_size_bytes " will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes (automatically reverted to 0)	50
class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than "class_tail_drop_large_packet_size_bytes ". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
class_tail_drop_large_packet_size_bytes	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop policy. If n=0, all packets treated as small packets. This value must be <= 1500.	No	0
class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to "class_tail_drop_large_packet_size_bytes " will have to wait in the class scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes	0
class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "class_tail_drop_large_packet_size_bytes ". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	0
class_dup_disable_depth_greater_ms	Number	Designates the amount of time a duplicate packet may wait in the queue before being discarded, which prevents duplicate	No	greater of class_tail_drop_s

		packets from consuming bandwidth when bandwidth is limited.		mall_packet_ms and class_tail_drop_large_packet_ms
class_dup_disable_depth_greater_bytes	Number	Defines the queue depth of the class scheduler at which point duplicate packets will begin being discarded.	No	128000
reassign_flow_if_packet_exceeds_size_bytes	Number	After a flow is established, if a packet that exceeds this size is detected on WAN ingress, then the flow will be moved to the class indicated below.	Only required if reassign_flow_if_packet_exceeds_size_class_id or reassign_flow_if_packet_exceeds_size_class_name is set.	2000
reassign_flow_if_packet_exceeds_size_class_id	Number	The class id of the class to which flows will be reassigned if the size above is exceed.	One and only one of these two parameters must be set if reassign_flow_if_packet_exceeds_size_bytes is set.	N/A
reassign_flow_if_packet_exceeds_size_class_name	Text	The class name of the class to which flows will be reassigned if the size above is exceed.		N/A
reassign_class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than “reassign_class_tail_drop_large_packet_size_bytes” will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes (automatically reverted to 0)	50
reassign_class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than “reassign_class_tail_drop_large_packet_size_bytes”. If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
reassign_class_tail_drop_large_packet_size_bytes	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop policy. If n=0, all packets treated as small packets. This value must be <= 1500.	No	0
reassign_class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to “reassign_class_tail_drop_large_packet_size_bytes” will have to wait in the class	No, not valid for bulk classes	0

		scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.		
reassign_class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "reassign_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	0
reassign_class_dup_disable_depth_greater_ms	Number	Designates the amount of time a duplicate packet may wait in the queue before being discarded, which prevents duplicate packets from consuming bandwidth when bandwidth is limited.	No	greater of reassign_class_tail_drop_small_packet_ms and reassign_class_tail_drop_large_packet_ms
reassign_class_dup_disable_depth_greater_bytes	Number	Defines the queue depth of the class scheduler at which point duplicate packets will begin being discarded.	No	128000
tcp_standalone_ack_class_id	Number	The class id of the class that will be used for standalone TCP ACKs. This has no effect on packets that are piggyback ACKs with payload.	No	class_id
tcp_standalone_ack_class_name	Text	The class name of the class that will be used for standalone TCP ACKs. This has no effect on packets that are piggyback ACKs with payload.	No	N/A
tcp_standalone_ack_class_tail_drop_small_packet_ms	Number	Defines the maximum amount of estimated time that packets smaller than "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler . If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes (automatically reverted to 0)	50
tcp_standalone_ack_class_tail_drop_small_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets smaller than "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be counted.	No	128000
tcp_standalone_ack_class_tail_dr	Number	Packets destined for this class which are >= n bytes will follow large packet drop policy, < n will follow small packet drop	No	0

op_large_packet_size_bytes		policy. If n=0, all packets treated as small packets. This value must be <= 1500.		
tcp_standalone_ack_class_tail_drop_large_packet_ms	Number	Defines the maximum amount of estimated time that packets larger than or equal to "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes" will have to wait in the class scheduler. If the estimated time exceeds this threshold, the packet will be discarded and statistics will be counted.	No, not valid for bulk classes	0
tcp_standalone_ack_class_tail_drop_large_packet_bytes	Number	Defines the maximum queue depth of the class scheduler for packets larger than or equal to "tcp_standalone_ack_class_tail_drop_large_packet_size_bytes". If the queue depth exceeds this threshold, the packet will be discarded and statistics will be	No	0

set wan_properties

Keyword	Type	Description	Required	Default
transmit_mode	Text	Select from the three available methods of transferring packets: Load balancing across multiple paths, duplicating across the two most unique paths, sending on a single persistent path.	No	load_balance_paths
retransmit_lost_packets	Boolean	This parameter specifies that flows matching this rule will be sent using reliable service to the remote appliance, and as such that any packets lost will be retransmitted.	No	no

set egress_properties

Keyword	Type	Description	Required	Default
resequence_packets	Boolean	Defines that traffic flows that match this rule should be tagged for sequence order, and the packets should be reordered (if necessary) at the WAN Egress appliance.	No	no
resequence_holdtime_ms	Number	Defines the maximum delay that a packet may be held awaiting re-sequence. When the timer expires the packet will be sent to the LAN without waiting any further for the pre-requisite sequence numbers.	No	If TCP: 900 If Non-TCP: 250
discard_late_resequence_packets	Boolean	After a packet's sequence timer has expired for a dependent packet, and the packets were permitted to the LAN: If a late packet does arrives at WAN egress, this property defines what is to be done with it.	No	Yes

Keyword	Type	Description	Required	Default
dscp_tag_value	Text	Defines a dscp tag that will be applied to packets that match this rule on WAN egress, before they are sent to the LAN.	No	N/A

set deep_packet_inspection_properties

Keyword	Type	Description	Required	Default
enable_passive_ftp_detection	Boolean	If enabled, will make processing decisions based upon user data.	No	Non-FTP rule->NO FTP rule->YES

add dhcp

add dhcp_subnet

Keyword	Type	Description	Required	Default
virtual_interface_name	Text	Name of virtual interface	Yes	N/A
domain_name	Text	Domain name that will be sent to the client	No	N/A
primary_dns	IP Address	primary dns that will be sent to the client	No	N/A
secondary_dns	IP Address	secondary dns that will be sent to the client	No	N/A
enabled	Boolean	if false then subnet not used	No	Yes

add dhcp_subnet_range

Keyword	Type	Description	Required	Default
range_start	IP Address	This is the first IP Address available for lease in this subnet range	Yes	N/A
range_end	IP Address	This is the last IP Address available for lease in this subnet range	Yes	N/A
gateway	IP Address	This is the advertised gateway for leases in this subnet range	No	N/A

Keyword	Type	Description	Required	Default
option_set_name	Text	This is a reference to a user defined dhcp_option_set. The referenced dhcp_option_set's options will be applied to this dhcp_subnet_range	No	N/A

add dhcp_subnet_host

Keyword	Type	Description	Required	Default
fixed_ip_addr	IP Address	If the dhcp server encounters the user defined mac_addr for this host, then assign that host the fixed_ip_addr	Yes	N/A
mac_addr	Mac Address	This is the mac address that the host will match against in order to assign the fixed_ip_addr	Yes	N/A

add dhcp_relay

Keyword	Type	Description	Required	Default
virtual_interface_name	Text	name of virtual interface that will be used for forwarding to server	Yes	N/A
server_ip	IP Address	ip address of dhcp server	Yes	N/A
server_ip2	IP Address	Optional second ip address of dhcp server	No	N/A
server_ip3	IP Address	Optional third ip address of dhcp server	No	N/A
server_ip4	IP Address	Optional fourth ip address of dhcp server	No	N/A

add lan_gre_tunnel

Keyword	Type	Description	Required	Default
tunnel_name	Text	GRE Tunnel Name	Yes	
src_ip	IP Address	Source IP Address Must be one of local Virtual Interface IP address. tunnel src ip must be valid VIP	Yes	
dest_ip	IP Address	Destination IP Address. tunnel src_ip, dest_ip pair must be unique for each LAN GRE tunnel	Yes	
tunnel_ip_addrn	Network Address	GRE Tunnel Network Address. Must be unique for each LAN GRE tunnel	Yes	
keepalive_period_s	Number	Keep alive period in seconds	No	10
keepalive_retries	Number	Kepp alive retries	No	3
checksum	Boolean		No	False

Keyword	Type	Description	Required	Default
routing_domain	Text	This is the routing_domain associated that this lan_gre_tunnel is associated with. Only traffic sourced/destined for the specified routing_domain may utilize this tunnel.	No	“
firewall_zone	Text	The Firewall Zone for the tunnel.	No	Default_LAN_Zone

add dns_proxy

set dns_proxy_properties

Keyword	Type	Description	Required	Default
routing_domain	Text	Routing domain name	Yes	N/A
primary_dns_server_ip	IP Address	Default primary DNS server IP. Note: Primary_dns_server_ip must be configured if primary_use_dhcp_client_dns is not set to yes.	No	N/A
primary_use_dhcp_client dns	Boolean	If set to yes, ignore primary dns server ip setting.	No	No
secondary_dns_server ip	IP Address	Default secondary DNS server IP	No	N/A
secondary_use_dhcp client dns	Boolean	If set to yes, ignore secondary dns server ip setting	No	No

Add overrider_dns_server

Keyword	Type	Description	Required	Default
rmatch_domain	Text	If defined, DNS query match this will be forwarded to the *_dns_server_ip.	Yes	N/A
primary_dns_server_ip	IP Address	Primary DNS server IP for DNS request match the match_domain.	Yes	N/A
secondary_dns_server_ip	IP Address	Secondary DNS server IP for DNS request match the match_domain.	No	N/A

set ipsec_properties

Keyword	Type	Description	Required	Default
enabled	Boolean	IPSec Enabled, yes|no	Yes	no
tunnel_type	Text	IPSec Encapsulation Type, esp|esp auth|ah	No	esp
encryption_mode	Text	IPSec Encryption mode, aes128|aes256	No	aes128
hash_algorithm	Text	sha|sha256	No	sha

Keyword	Type	Description	Required	Default
lifetime_s	Integer	Defines the lifetime (in seconds) of the keys for ipsec (phase 2). Valid values are 0-86400.	No	28800

Conduit Default Set

The conduit_default_set allows the user to define a conduit's rule defaults, rules and classes and then apply them in the add conduit_service command in add appliance. This is similar to redefining rules and classes using a macro, however this allows the classes and rules to be declared and audited in one central location.

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define conduit_default_set name=text
{
      advanced_properties
            [activate_standby_bandwidth_threshold_percentage=1...200]
set ipsec_properties
                  enabled = [yes|no]
                  tunnel_type = [esp|esp_auth|ah]
                  encryption_mode = [aes128|aes256]
                  hash_algorithm = [sha|sha256]
                  lifetime_s = [0...86400];
            [set realtime class]
                  class_id=n
                  [initial_rate_kbps=n | initial_rate_pct=p ]
                  sustained_rate_kbps=n | sustained_rate_pct=p
                  [initial_period_ms=n] ;

            [set interactive class]
                  class_id=n
                  [initial_share_pct=p]
                  sustained_share_pct=p
                  [initial_period_ms=n] ;

            [set bulk class]
                  class_id=n
                  [bulk_share_pct=p]
                  [delay_min_depth_bytes=n];

            [add rule]
            {
                  [set properties]
                        [precedence={high | medium | low}]
                        [application_name=text]
                        [track_performance={yes | no}]
```

```
                    [override_service={passthrough | internet | intranet | discard}] ;

            set match_criteria
                    [ip_addrn=x.x.x.x/n]
                    [src_ip_addrn=x.x.x.x/n]
                    [dst_ip_addrn=x.x.x.x/n]
                    [port_num=n-n]
                    [src_port=n-n]
                    [dst_port=n-n]
                    [ip_protocol_num=n]
                    [ip_dscp=aaxx]
                    [ip_tos_match_flows={yes | no}]
                    [rouing_domain=text]
                    [vlan_id={native | 0...4094}]
                    [protocol_str={ * | FTP | SMTP | HTTP | TELNET | ICMP |
HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

            [set traffic_optimization_properties]
                    [enable_tcp_termination={yes | no}]
                    [enable_wan_op={yes | no}]
                    [enable_packet_aggregation={yes | no}];

            [set ingress_properties]
                    [class_id=n]
                    [class_name=text]
                    [class_tail_drop_small_packet_ms=n]
                    [class_tail_drop_small_packet_bytes=n]
                    [class_tail_drop_large_packet_size_bytes=n]
                    [class_tail_drop_packet_ms=n]
                    [class_tail_drop_packet_bytes=n]
                    [class_dup_disable_depth_greater_ms=n]
                    [class_dup_disable_depth_greater_bytes=n]
                    [reassign_flow_if_packet_exceeds_size_bytes=n]
                    [reassign_flow_if_packet_exceeds_size_class_id=n]
                    [reassign_flow_if_packet_exceeds_size_class_name=text]

        [reassign_class_tail_drop_small_packet_ms=n]
                    [reassign_class_tail_drop_small_packet_bytes=n]
                    [reassign_class_tail_drop_large_packet_size_bytes=n]
                    [reassign_class_tail_drop_packet_ms=n]
                    [reassign_class_tail_drop_packet_bytes=n]
                    [reassign_class_dup_disable_depth_greater_ms=n]
                    [reassign_class_dup_disable_depth_greater_bytes=n]
                    [tcp_standalone_ack_class_id=n]
                    [tcp_standalone_ack_class_name=text]

            [tcp_standalone_ack_class_tail_drop_small_packet_ms=n]
                    [tcp_standalone_ack_class_tail_drop_small_packet_bytes=n]

        [tcp standalone ack class tail drop large packet size bytes=n]
```

```
                        [tcp_standalone_ack_class_tail_drop_packet_ms=n]
                        [tcp_standalone_ack_class_tail_drop_packet_bytes=n];

                set wan_properties
                        [transmit_mode={load_balance_paths | duplicate_paths |
persistent_path}]
                        [retransmit_lost_packets={yes | no}];

                set egress_properties
                        [resequence_packets={yes | no}]
                        [resequence_holdtime_ms=n]
                        [discard_late_resequence_packets={yes | no}]
                        [dscp_tag_value=aaxx];

                [set deep_packet_inspection_properties]
                        [enable_passive_ftp_detection={yes | no}] ;
        }
}
```

Commands and Parameters

Keyword	Type	Description	Required	Default
name	Text	The name to be used when referencing this default set through the configuration and user interfaces.	Yes	N/A

Intranet Default Set

The internet_default_set allows the user to define an intranet service with properties, routes and rules and then apply them in the add intranet_service command in add appliance. This is similar to redefining routes and rules using a macro, however this allows the classes and rules to be declared and audited in one central location.

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define intranet_default_set name=text
{
        [set properties]
                [primary_reclaim={yes | no}];

        [add rule]
        {
                set properties
                        [precedence={high | medium | low}]
                        [application_name=text]
                        [override_service={passthrough | internet | discard}];

                set match_criteria
                        [ip_addrn=x.x.x.x/n]
                        [src_ip_addrn=x.x.x.x/n]
                        [dst_ip_addrn=x.x.x.x/n]
                        [port_num=n-n]
                        [src_port=n-n]
                        [dst_port=n-n]
                        [ip_protocol_num=n]
                        [ip_dscp=aaxx]
                        [ip_tos_match_flows={yes | no}]
                        [rouing_domain=text]
                        [vlan_id={native | 0...4094}]
                        [protocol_str={ * | FTP | SMTP | HTTP | TELNET | ICMP |
HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

                [set deep_packet_inspection_properties]
                        [enable_passive_ftp_detection={yes | no}] ;
        }
} // intranet
```

Commands and Parameters

Refer to previous sections for parameter details.

Internet Default Set

The internet_default_set allows the user to define an internet service with properties, routes and rules and then apply them in the add internet_service command in add appliance. This is similar to redefining routes and rules using a macro, however this allows the classes and rules to be declared and audited in one central location.

Syntax

Note: All parameters listed in square brackets [] are optional.

```
define internet_default_set name=text
{
```

```
                [set properties]
                        [primary_reclaim={yes | no}];

                [add rule]
                {
                        set properties
                                [precedence={high | medium | low}]
                                [application_name=text]
                                [override_service={passthrough | intranet | discard}];

                        set match_criteria
                                [ip_addrn=x.x.x.x/n]
                                [src_ip_addrn=x.x.x.x/n]
                                [dst_ip_addrn=x.x.x.x/n]
                                [port_num=n-n]
                                [src_port=n-n]
                                [dst_port=n-n]
                                [ip_protocol_num=n]
                                [ip_dscp=aaxx]
                                [ip_tos_match_flows={yes | no}]
                                [rouing_domain=text]
                                [vlan_id={native | 0...4094}]
                                [protocol_str={ * | FTP | SMTP | HTTP | TELNET | ICMP |
        HTTPS | SSH | RTP | RTCP | DHCP | DNS | SNMP | NFS | CIFS | TCP | UDP}];

                        [set wan_properties]
                                [wan_link_name=text];

                        [set deep_packet_inspection_properties]
                                [enable_passive_ftp_detection={yes | no}] ;
                }

        } // internet
```

Commands and Parameters

Refer to previous sections for parameter details.

Sample Configuration File

```
//**************************************
//ncn - raleigh
//**************************************

define site name=raleigh
{
        add appliance
        name=primary {
                set appliance_properties
                        model=t3000
                        secure_key=0xcafe0004beef5533
                        appliance_mode=primary_ncn
                        default_direct_route_cost=6;

                add interface_group
                {
                        set properties
                                bypass_mode=fail_to_block;

                        add ethernet_interface device=1;
                        add  virtual_interface  name=vlan1  vlan_id=100;
                        add  virtual_interface  name=vlan2  vlan_id=200;
                        add virtual_interface name=vlan3 vlan_id=native;
                }

                add interface_group
                {
                        set properties
                                secure_zone=untrusted
                                bypass_mode=fail_to_block;

                        add ethernet_interface device=4;
                        add virtual_interface name=vlan4 vlan_id=native;
                }

                add virtual_ip_addrn virtual_interface_name=vlan1
ip_addrn=192.168.50.6/24;

                add virtual_ip_addrn virtual_interface_name=vlan2
ip_addrn=192.168.51.6/24;

                add virtual_ip_addrn virtual_interface_name=vlan3
ip_addrn=192.168.52.6/24;
```

```
add route
        net=192.168.0.0/16
        gw_ip_addr=192.168.50.5
        cost=7
        service=local;



add conduit_service remote_site_name=sjc
{
        set interactive_class
                class_id=1
                class_name=udp_class
                initial_share_pct=12
                sustained_share_pct=12;

        set interactive_class
                class_id=2
                class_name=class_2
                initial_share_pct=12
                sustained_share_pct=12;

        set bulk_class
                class_id=3
                class_name=class_3
                bulk_share_pct=100;

        add rule
        {
                set match_criteria
                        protocol_str=udp;

                set properties
                        precedence=low;

                set ingress_properties
                        class_name=udp_class;

                set wan_properties
                        transmit_mode=duplicate_paths
                        retransmit_lost_packets=true;

                set egress_properties
                        resequence_packets=true;
        }
}
add internet_service
{
}
```

```
                add virtual_wan_link name=raleigh-t1
                {
                        add access_interface name=raleigh-t1-accessint0
                                virtual_interface_name=vlan1
                                virtual_ip_addr=192.168.50.66
                                gw_ip_addr=192.168.50.1;
                        set properties
                                primary_conduit_access_interface=raleigh-t1-accessint0
                                wan_ingress_physical_rate_kbps=1444
                                wan_egress_physical_rate_kbps=1444
                                wan_ingress_permitted_rate_kbps=1444
                                wan_egress_permitted_rate_kbps=1444
                                public_ip_addr=224.54.13.54;
                        add conduit_usage
                                remote_site_name=sjc
                                wan_egress_rate_fair_share=800000
                               wan_ingress_rate_fair_share=800000
                               service_group_name=default
                               wan_egress_minimum_reserved_bandwidth_kbps=200
                               wan_ingress_minimum_reserved_bandwidth_kbps=200;
                               add net_usage
                                 service_type=internet
                                 wan_egress_rate_fair_share=200000
                              wan_ingress_rate_fair_share=200000
                              service_group_name=default; add
                              service_group
                                 name=default
                                 wan_egress_rate_fair_share=1000000
                                 wan_ingress_rate_fair_share=1000000;
                }


        }
        add ha_appliance name=secondary;
        add ha_service
        {
                set properties
                        primary_appliance_name=primary
                        secondary_appliance_name=secondary;
                add interface_group
                {
                        set interface_properties
                                virtual_interface_name=vlan1
                                primary_ip_addr=192.168.50.101
                                secondary_ip_addr=192.168.50.102;
                }
        }
}
```

```
//****************************************
//site - sjc
//****************************************

define site name=sjc
{
        add appliance name=talari
        {
                set appliance_properties
                        model=t730
                         secure_key=0xcafe7777cafe7777;

                add interface_group
                {
                        set properties
                                bypass_mode=fail_to_wire;

                          add ethernet_interface device=1;
                          add ethernet_interface device=2;
                        add virtual_interface name=vlan1 vlan_id=100;
                        add bridge_pair
                                device_one=1
                                device_two=2;
                }

                add virtual_ip_addrn virtual_interface_name=vlan1
ip_addrn=192.168.61.6/24;



                  add conduit_service remote_site_name=raleigh
                {
                }

                add virtual_wan_link name=sjc-cbl
                {
                        add access_interface name=sjc-cbl-accessint0
                                virtual_interface_name=vlan1
                                virtual_ip_addr=192.168.61.6
                                gw_ip_addr=192.168.61.1;
                        set properties
                                primary_conduit_access_interface=sjc-cbl-accessint0
                                wan_ingress_physical_rate_kbps=4000
                                wan_egress_physical_rate_kbps=20000
                                wan_ingress_permitted_rate_kbps=4000
                                wan_egress_permitted_rate_kbps=20000
                                enable_public_ip_learning=true;
                        add conduit_usage
                                remote_site_name=raleigh
                                wan_egress_rate_fair_share=200000
```

```
                                        wan_ingress_rate_fair_share=200000
                                        service_group_name=default
                                        wan_egress_minimum_reserved_bandwidth_kbps=100
                                        wan_ingress_minimum_reserved_bandwidth_kbps=100;
                                add service_group
                                        name=default
                                        wan_egress_rate_fair_share=1000000
                                        wan_ingress_rate_fair_share=1000000;
                        }
                }
        }
```

Appendix A: Port Definitions for Applications

Protocol	Port(s) Used
CIFS (TCP)	137, 139, and 445
CIFS (UDP)	137-138
DHCP (UDP)	67-68
DNS Protocols (TCP and UDP)	53
FTP (TCP)	20-21
HTTP (TCP)	80, 8080, and 8008
HTTPS (TCP)	443
ICMP	—
NFS Protocols (TCP and UDP)	2049
RTP (UDP)	5004
RTCP (UDP)	5005
SMTP (TCP)	25, 110, and 366
SNMP Protocols (TCP and UDP)	161-162
SSH (TCP and UDP)	22
TCP	—
Telnet (TCP)	23 and 107
UDP	—