CLOUD INFRASTRUCTURE NETWORK AND SECURITY USER GUIDE
WELCOME TO THE NETWORK AND SECURITY USER GUIDE

This guide focuses on the network and security features of cloud infrastructure, common to all virtual server types. It describes the physical environment we use to deliver your cloud services, as well as additional network and security features you can control.

This guide should be read in conjunction with other Cloud Services guides. See How to use this guide for details.

AUSTRALIAN ACCOUNT HOLDERS

For sales, account set-up enquiries and technical support, contact your Telstra representative or visit the Cloud Services website (www.cloud.telstra.com), where you’ll find all our contact details plus a glossary, FAQs and Our Customer Terms.

TELSTRA GLOBAL ACCOUNT HOLDERS

For sales, account set-up enquiries and technical support, contact your Telstra Global representative or visit the Telstra Global website (www.telstraglobal.com/cloud) for the customer service team in your region.

Note: we don’t provide assistance with issues specific to a customer’s local network, servers, operating systems and software (post-installation). Specialist technical support may be charged as an additional service.

CONVENTIONS USED IN THIS GUIDE

The following typographical conventions are used in this guide for simplicity and readability:

Web addresses, email addresses and hyperlinks are shown in bold italics, for example www.cloud.telstra.com.

Button names and titles/features on your computer screen are shown in italics.

User input is shown in typewriter font.
WHAT’S INSIDE

CHAPTER 1  HOW TO USE THIS GUIDE  4
CHAPTER 2  OUR DATA CENTRES  6
CHAPTER 3  HOW WE DELIVER CLOUD SERVICES  9
CHAPTER 4  YOUR VIRTUAL DATA CENTRES  11
CHAPTER 5  VIRTUAL SERVER NETWORKS AND SECURITY  13
CHAPTER 6  YOUR PUBLIC NETWORK  17
CHAPTER 7  YOUR PRIVATE NETWORK  18
CHAPTER 8  TELSTRA NEXT IP® NETWORK (GLOBAL IP VPN)  24
CHAPTER 9  IPSEC VPN  25
CHAPTER 10  VLAN EXTENSION  28
CHAPTER 11  DUAL NETWORK CONNECTION  37
CHAPTER 12  FIREWALLS  39
CHAPTER 13  LOAD BALANCERS  45
CHAPTER 14  MANAGEMENT CONNECTION TO A VIRTUAL SERVER  48
CHAPTER 15  SMTP MAIL RELAY  51
CHAPTER 16  APPENDIX A: STATIC ROUTING PRIVATE TRAFFIC  53
CHAPTER 17  APPENDIX B: VLAN EXTENSION CSR DEVICE CONFIGURATION  55
CHAPTER 1
HOW TO USE THIS GUIDE

The network and security environment is common to all virtual server types within cloud infrastructure. You can use this guide as a supplement to any of the following guides, which deal with specific virtual server types:

- Virtual Server (Shared) User Guide
- Virtual Server (Dedicated) User Guide
- Managed Virtual Server (Dedicated) User Guide

This guide includes instructions on how to create and modify virtual server network connections and security features. The guide assumes you have access to the Cloud Services management console – for more information about using the Cloud Services management console, see any of the virtual server user guides listed above.

For details about managing your account and accessing the Cloud Services management console, see the Account Management Guide.
Our Cloud Services diagram below shows what’s covered in this guide, and where to go for further details.
Our data centres securely house the physical resources and infrastructure used to provide our cloud solutions. We own, operate and maintain all our physical data centres. Data centres are currently located in:

**Australian locations**
- Melbourne
- Perth
- Sydney

**International locations**
- Singapore
- Hong Kong
- London

The physical infrastructure within our data centres is protected by four layers of security:
- Outer perimeter
- Site grounds
- Buildings (including electronically-secured floors and CCTV corridor surveillance)
- Internal rooms (including CCTV surveillance for rooms hosting ICT infrastructure and locked cabinets and cages)

Data centres provide you with connectivity to:
- The internet
- Your private networks via a Telstra Next IP® network, Global IP VPN connection or IPsec VPN tunnel
- Your stored data
- Both dedicated and shared virtual servers and resources

You can select which data centre(s) you will use to source cloud infrastructure services. We describe your chosen source as your *virtual data centre*. You’ll find instructions for managing your *virtual data centres* later in this guide.

If you’re drawing your cloud resources from Australia, your virtual servers (shared) can only be provisioned from our Melbourne data centre. All other virtual server types and resources are available from any of our data centres in Australia and globally.

Our *backup* service uses separate data centres for short-term storage and long-term retention.
**AVAILABILITY AND RELIABILITY**

Our data centre infrastructure is fully redundant to protect your services and data from a single point-of-failure.

This enables us to provide cloud services with high levels of availability, service support and coverage. Infrastructure is continuously monitored by our Cloud Services support team using advanced monitoring tools and denial of service protection.

Network reliability is maintained by redundancy on two levels:

- **Intra-component redundancy** - including dual supervisor engines, multiple power supplies served by diverse power sources and fan redundancy
- **Inter-component redundancy** - including dual physical components and multiple links

Service level agreements can be viewed in *Our Customer Terms* (Australian customers only) or your separate agreement with us.

**NETWORK SECURITY**

All our data centres are located in or close to capital cities, and housed in high security physical environments. Your data is protected 24/7 by our team of security specialists. The role of our Cloud Services support team is to provide:

- Protection of the physical infrastructure that provides your cloud services
- Privacy and security of individual customer’s data in a multi-tenancy environment
- Basic security controls at the infrastructure and network level
- Infrastructure logging, alerting and auditing

Some of the security features of our cloud services infrastructure include:

- Network-based firewalls
- Remote access security
- Regular vulnerability checks
- Denial of service protection
- Privacy controls

Our cloud infrastructure is protected by a sophisticated intrusion detection and prevention system (IDS/IDP) and a firewall protecting the entire cloud infrastructure perimeter.

To maintain security standards, we use leading technologies to perform regular network and infrastructure security updates. We also perform regular penetration testing of our platform using a third party.

In addition to the security measures our infrastructure provides, we offer ways for you to customise and enhance your own *cloud network security*.

**CUSTOMER ISOLATION**

Your data and virtual resources are separated from other customers on three layers – network, compute and data.

*Network isolation* is achieved using technology that ensures low-level network separation, and uses advanced and encrypted communication channels (e.g. SSL VPN). Transit networks between customers’ virtual servers and data storage areas are isolated and unreachable from any network.
**Compute isolation**

For virtual server (shared), compute isolation occurs at the hypervisor level. Separate customer identities are maintained, and strong access controls ensure that customers can only access the resources allocated to them. We enforce operational separation of duties and strict change controls that govern all customer configurations.

For virtual server (dedicated) and managed virtual server (dedicated), separation occurs at the physical hardware level within our data centres.

**Data isolation**

For virtual server (shared), data isolation is maintained by completely encapsulating your virtual server environment (including stored data) in a single file that is unreachable to anything other than your own virtual servers.

For virtual server (dedicated) and managed virtual server (dedicated) we dedicate entire volumes to a single customer to achieve data isolation.
CHAPTER 3
HOW WE DELIVER CLOUD SERVICES

The physical infrastructure we use to provide cloud services is based on multi-tenancy architecture and designed to give you flexibility, and ensure security, privacy and reliability.

We use two network constructs, public and private. These following diagrams provide a simplified view of how these networks operate when accommodating multiple customers.

The logical routing instance is part of our infrastructure, not visible or configurable by you.

PUBLIC NETWORK

Our public network provides your virtual servers with access to the internet, via a public interconnect.

In the public network, virtual servers are allocated individual IP addresses on a shared subnet. Your virtual servers may share the same subnet as virtual servers from other customers.

Security separation between your virtual servers can be achieved by adding a firewall. You have the option of adding network services such as load balancers.
PRIVATE NETWORK

Our private network allows you to access virtual servers in your private network, via a private interconnect, through a private network connection.

The private network provides your own logical routing instance to which you can add private IP subnets.

Security separation between your virtual servers can be achieved by adding a firewall. You have the option of adding network services such as load balancers.
A virtual data centre represents the collection of cloud resources you’re drawing from a specific physical location. A single virtual data centre also represents a logically-isolated network within your cloud solution. Each of your virtual data centres can be viewed as a network configuration diagram, in the Network & security page of the management console.

MULTIPLE VIRTUAL DATA CENTRES

Cloud infrastructure lets you draw your cloud resources from multiple data centres in different locations and assign resources to your choice of virtual data centre.

You can create multiple virtual data centres drawing resources from the same physical data centre location. If you choose to do this, each virtual data centre will form a logically-isolated network with its own private interconnect. By default these virtual data centres will have no communication between each other. Separate firewalls, load balancers and network connections will be required for each virtual data centre.

Your cloud solution can include virtual data centres from any of our locations around the world. Virtual server (shared) is not available in all Australian virtual data centre locations – only Melbourne.
Multiple virtual data centres could be used for several reasons – you may want to:

- Add virtual server (shared) if it’s not available from your current data centre
- Strategically locate specific cloud resources closer to where the end-users are based

**ADD A VIRTUAL DATA CENTRE**

You can add a new virtual data centre at any time by purchasing a new compute service.

**RENAME A VIRTUAL DATA CENTRE**

You can customise the name of a virtual data centre to make the name more meaningful to your operations.

**REMOVE A VIRTUAL DATA CENTRE**

A virtual data centre will be removed after you remove all the compute services it contains.

**NOMINATE A DATA CENTRE**

If your cloud solution is contained within a single virtual data centre, then your resources will be automatically assigned to that virtual data centre.

But if you’re operating your cloud solution across multiple data centre locations, you’ll be asked where you want to assign certain cloud resources as you add them, such as:

- SSL VPN users
- SMTP mail relay

Other types of resources can only be created from within a specific virtual data centre environment.

- Firewalls
- Load balancers
- Private network connections

Each of your virtual data centres can be viewed in the Cloud Services management console as a network diagram. These diagrams provide an alternative way of adding virtual servers, resources, and network connections to your existing configuration. Select the item on the diagram you want to configure, and the fields required to add the item will appear on screen.
You can choose to connect a virtual server to a public or private network, or use dual homing to connect a virtual server to both networks.

Each of your networks can contain virtual servers and associated firewalls and load balancers. All virtual servers within a network can be allowed to communicate with each other, or separated using firewall rules.
CLOUD INFRASTRUCTURE NETWORK FEATURES

There are a number of features you can customise to manage traffic flow, privacy and security of your data. Apart from internet access, all network features are optional and inactive by default.

Many of these features are described in detail, later in this guide.

To view pricing of optional network features, refer to the pricing guide for your data centre location.

**Dual homing** allows a single server to be accessed via both public and private network connections, and communicate with virtual servers in both your public and private networks.

**SSL VPN connection** is a way to remotely and securely manage individual virtual servers. **Firewalls** can be configured by you to allow or deny traffic through groups or individual virtual servers. A separate firewall is required for each network, and each compute service within your cloud solution.

**Load balancers** can be used to distribute traffic across multiple virtual servers within the same network.

**Security add-ons** are optional features available to enhance your network security.

**SMTP mail relay** is an optional service allowing you to send outbound email from a virtual server in the cloud.

**VLAN Extension** allows you to extend a subnet between your own network environment and Telstra cloud infrastructure in an Australian virtual data centre, greatly simplifying server migration and enabling hybrid cloud environments.
NETWORK SECURITY ADD-ONS

These optional network security add-ons can be added to your cloud solution at any time, to maximise the security of your cloud resources and data.

For more information including pricing, see the Pricing Guide for your virtual data centre location.

INTERNET PROTECTION

*Internet protection (email)* helps keep spam, viruses and inappropriate content off your network. You can choose to have anti-virus and anti-spam filtering software applied to virtual servers connected to the internet and hosted mail servers. The software scans incoming emails to detect spam and viruses.

*Internet protection (web)* helps shield your business from known and emerging viruses and web threats including malware and spyware. Web filtering can be applied to virtual servers in your public network and hosted proxy servers.

VULNERABILITY DISCOVERY

Vulnerability discovery scans virtual servers in your public networks to identify and prioritise potential weak points and security exposures. The report produced during the scan details and assigns criticality ratings to any exposure detected per-server.

DENIAL OF SERVICE (DOS) PLATFORM PROTECTION

Our Cloud Services platform is shared and as such a DoS attack on one customer could affect the platform and performance of other customers if left unmanaged. As a standard feature, Telstra’s Security Operations Centre monitors the platform internet traffic. If unusual traffic is detected we automatically rate limit the traffic to ensure continued performance of other customers. We’ll notify you if your virtual servers are attacked and your internet connection has been rate limited.

We’ll keep you informed by:

- Emailing you to inform you of the attack, and potential reduction in your service performance
- Emailing you when the attack has passed, and normal service performance can resume

DoS platform protection is included with your cloud services and requires no activation on your part. This level of protection is provided in all virtual data centre locations. You can’t remove or configure this standard level of protection, however if using any of our Australian virtual data centre locations, you have the option of purchasing our DoS protection service.

DENIAL OF SERVICE PROTECTION

Denial of service protection is an optional premium service to prevent malicious attacks across your cloud solution.

In the event of an attack traffic is diverted to Telstra’s Security Operations Centre where it is cleaned before being routed back to your virtual data centre.

More information about this service is available on the Telstra [website](#).
NETWORK CONFIGURATION

A wide range of network configurations are made possible using combinations of:

- Firewalls
- Routing
- Load balancers
- Private IP subnets
- Network connections
- Virtual data centres

Virtual server networks can be configured in multiple tiers and zones.

Refer to the *Infrastructure Design Guide* to see examples of how common network scenarios can be built using our cloud solution.
VIRTUAL SERVERS

Virtual servers in your public network are connected to the internet by default, via your public interconnect. No network address translation is required.

FIREWALLS

To maintain security from the outset, we strongly recommend configuring a firewall in your public network before creating any virtual servers. See the firewalls section of this guide for further information.

Each compute service requires a separate firewall.

IP ADDRESSING

We allocate public IP addresses to virtual servers in your public network, from a shared subnet on a one-by-one basis as you need them. Public IP addresses could be automatically allocated - or you may need to request them - depending on the type of virtual server. Check your relevant virtual server user guide for instructions.

The IP addresses we allocate to your virtual servers in the public network won’t be sequential. All public IP addresses allocated to virtual servers are static.

Once provided, you can’t move your IP addresses to another server. IP addresses should not be manually changed. Modifying the IP addresses assigned to a virtual server’s internet vNIC could cause connection to your public interconnect and internet, to be lost.

NETWORK RESOURCES

All of our cloud infrastructure network features are available for use within your public network.

LOAD BALANCING

A single load balancer can distribute traffic across multiple virtual servers in any combination of server type, within your public network. We provide a public IP address for the load balancer. The load balancers section of this guide contains further information.
Connect to your private network virtual servers (via your private interconnect) through either:

- a Telstra Next IP® network
- Global IP VPN
- IPsec VPN tunnel

A private network must be created before it can be populated with virtual servers, firewalls or a load balancer.

Private IP subnets are nominated by you. All private IP addresses allocated to virtual servers are static.

In addition to the network security add-ons that can be added to your cloud solution, there are also a number of network resources you can add to your network at any time.

The following network and security features can be deployed and customised through the Cloud Services management console. The Network & security management section is located under Infrastructure in the Cloud Services management console. From here, you can:

- Create a private network
- Remove a private network
- Create private IP subnets and allocate private IP addresses
- Extend an IP subnet over a VLAN Extension tunnel
- Modify your private network
- Connect to your private network through a Telstra Next IP® network (Global IP VPN)
- Connect to your private network through an IPsec VPN tunnel
- Add a second network connection to a virtual server
- Add and configure firewalls
- Add and configure load balancers
- Assign SSL VPN users
- Set up a SMTP mail relay
MAKING CHANGES TO YOUR NETWORK CONFIGURATION

In general, any changes, additions or removal of network resources can be made by completing a brief online request form through the Cloud Services management console. There are various forms available to deal with specific types of request.

After you fill out and submit a form, we’ll get to work processing your request. Each request form states the time it takes for us to make the particular addition or changes to your service.

We may get in contact with you if we need more information to process your service request, or if some of the information you provided in the form is incorrect. We’ll contact you using the details stored in your Telstra account, unless you provided us with an alternative contact when you submitted the request.

You can track a service request in the activity log, accessed from the Cloud Services management console’s reports section.

You can choose to create a private network in your cloud solution to contain all your virtual servers accessible through an IPsec VPN tunnel, Telstra Next IP® network or Global IP VPN connection.

A private network must exist before you can:

- Create virtual servers within a private network
- Establish a private network connection

Creating a private network involves an online request from you, and configuration by us before your private network becomes active.

You can separate and distinguish groups of virtual servers within a private network by using **private IP subnets**.

PRIVATE IP SUBNETS

A private IP subnet enables you to connect to your virtual servers within a private network, and access our cloud infrastructure via your private interconnect. You’ll need to provide a private IP subnet for each compute service.

The subnets you assign to different virtual server types within the same private network can’t overlap.

You can choose private IP subnets (non-internet addressable) for virtual server groups in your private network.

We currently only support IPv4 addresses. The IP subnet must come from the following RFC 1918 address ranges:

- 10.0.0.0 – 10.255.255.255
- 172.16.0.0 – 172.31.255.255
- 192.168.0.0 – 192.168.255.255

To make sure you have enough IP addresses to add as many virtual servers as you need in the future, we suggest you provide an IP subnet mask of at least /23.

Your cloud infrastructure private IP subnets may be able to be extended into your on-premises infrastructure, using **VLAN Extension**. Before doing this, make sure there will be no IP addresses replicated in both infrastructure environments. Reassign individual IP addresses where necessary.
We reserve the first three useable IP addresses of each subnet. The table below highlights the IP address capacity of various subnet masks:

<table>
<thead>
<tr>
<th>IP SUBNETS</th>
<th>AVAILABLE IP ADDRESS</th>
<th>AVAILABLE IP ADDRESSES</th>
</tr>
</thead>
<tbody>
<tr>
<td>/23</td>
<td>255.255.254.0</td>
<td>507</td>
</tr>
<tr>
<td>/24</td>
<td>255.255.255.0</td>
<td>251</td>
</tr>
<tr>
<td>/25</td>
<td>255.255.255.128</td>
<td>123</td>
</tr>
<tr>
<td>/26</td>
<td>255.255.255.192</td>
<td>59</td>
</tr>
<tr>
<td>/27</td>
<td>255.255.255.224</td>
<td>27</td>
</tr>
<tr>
<td>/28</td>
<td>255.255.255.240</td>
<td>11</td>
</tr>
</tbody>
</table>
CREATE A NEW PRIVATE NETWORK

If you intend to use our VLAN Extension service, create your new private network via the **VLAN Extension** request form in the Cloud Services management console, at the same time you extend your subnet(s).

**CHOOSE A COMPUTE SERVICE**

Select the compute service you’d like to add to your private network.

Choose one option from your existing compute services.

Select the virtual server type (shared, dedicated, or managed dedicated) you would like your private IP subnet to apply to. A separate private subnet is required for each compute service contained within your private network.

**SPECIFY YOUR PRIVATE IP SUBNETS**

Add one or multiple private IP subnets.

You’ll need to configure at least one private IP subnet to create a private network. You can also add more IP subnets in the future if you require them, using the process explained below.

You can create private IP subnets through the *Networks* section of the management console.

**IF CONNECTING TO YOUR PRIVATE NETWORK VIA TELSTRA NEXT IP® NETWORK**

If you’ve previously connected a Telstra Next IP® network to your virtual data centre, then at this point you can choose to make your private IP subnets accessible to your Telstra Next IP® network. You can modify this later through the *Telstra Next IP® network* section of the *Connections* page in the Cloud Services management console.

**ADD A FIREWALL**

At this point you have the option of adding a firewall to your private network. See the *firewalls* chapter of this guide for more details.
ALLOCATING IP ADDRESSES TO VIRTUAL SERVERS IN YOUR PRIVATE NETWORK

Individual IP addresses need to be allocated to every virtual server in your private network. You can allocate IP addresses when you create or dual home a virtual server.

Virtual server IP addresses must fall within a private IP subnet range configured in the private network. We reserve the first three useable IP addresses of each subnet to configure your network.

All private IP addresses allocated to virtual servers in cloud infrastructure are static.

If you change the virtual server’s IP address through the operating system, the Cloud Services management console will continue to display the original IP address.
MANAGE YOUR PRIVATE NETWORK

There are a number of ways to modify and manage your private network, after it’s initially created.

VIEW PRIVATE IP SUBNETS

You can view the original MAC and IP addresses for each of your private network connections through the management console. If you’ve chosen to manually change an IP address through the virtual server’s operating system, the new IP address will not be updated in the management console.

From this point in the Cloud Services management console you can also modify a virtual server’s network connections.

ADD IP SUBNETS TO AN EXISTING PRIVATE NETWORK

To add a private IP subnet, see the previous instructions in the Create a private network section.

Creating additional private IP subnets and configuring firewall rules around them, is a way to group and separate virtual servers within your private network. For examples of how you might do this, see the Infrastructure Design Guide.

To access virtual servers connected to a private IP subnet via an IPsec VPN tunnel, the IP subnet will need to be specified as one of your destination subnets when configuring an IPsec VPN tunnel.

To add a new IP subnet, provide both the IP subnet and the IP range within that subnet. See the previous Create a private network section for detailed instructions.

EXTEND AN IP SUBNET BETWEEN INFRASTRUCTURE ENVIRONMENTS

VLAN Extension allows you to extend a subnet between your own network environment and Telstra cloud infrastructure in an Australian virtual data centre, to transition servers between environments and enable hybrid cloud environments.

There are a few preconditions you’ll need to request this service. See the VLAN Extension chapter for details.

When you’re ready, you can request and partially configure VLAN Extension through the Connections page in the Cloud Services management console.

REMOVE AN IP SUBNET

Before you can remove a subnet, you’ll need to remove any virtual servers that were connected to this subnet when the server was first created.

Select the Remove subnet link.

REMOVE A PRIVATE NETWORK

Before you can remove a private network, you’ll need to remove any virtual servers, subnets, firewalls and load balancer that were connected to this network when the server was first created.

Select the Remove network link.
A Telstra Next IP® network connection (or Global IP VPN for virtual data centres located outside Australia) provides a permanent and secure way to connect your local area networks to your cloud solution (via your private interconnect).

You can use your existing IP MAN, Connect IP, Business IP or Global IP VPN network to access virtual servers in your private networks.

A separate Telstra Next IP® network connection is required for each virtual data centre you wish to privately communicate with. Multiple private network connections will allow communication between private interconnects in multiple virtual data centres. Multiple virtual data centres can communicate with one another when each one is connected to the same Telstra Next IP® network.

A Telstra Next IP® network connection can only be provided to your office locations within Australia. If you’re using a global data centre (Hong Kong, Singapore, London) then you can use the Global IP VPN connection method - the international equivalent to a Telstra Next IP® network.

Note: all Telstra Next IP® network references in this guide use the example of an Australian-based private network connection. If you’re using a global data centre, the Cloud Services management console will display Global IP VPN in place of Telstra Next IP® network.

**CONNECT TO YOUR TELSTRA NEXT IP® NETWORK**

You can connect to your Telstra Next IP® network from the Connections page in the Cloud Services management console. You can choose which of your IP subnets and private load balancer virtual IP addresses you’d like to make accessible to your Telstra Next IP® network connection. Only virtual servers and load balancers with IP addresses within the subnet range(s) you select will be accessible through your Telstra Next IP® network connection.

Subnets and load balancers which you’ve recently requested can only be selected once they are active. You can modify this configuration once the Telstra Next IP® network connection is active.

**DISCONNECT FROM YOUR TELSTRA NEXT IP® NETWORK**

You can disconnect from your Telstra Next IP® network by selecting the Disconnect link.
CHAPTER 9
IPSEC VPN

IPsec VPN provides a permanent, site-to-site network tunnel between an external network (such as your office network) and the private interconnect within a single virtual data centre. Data is transferred over the internet, through a private and secure network tunnel.

Before you can request an IPsec VPN tunnel, you'll need an active *private network*.

An IPsec VPN tunnel has two connected endpoints – one endpoint at your *source* site, usually your office LAN, and a *destination* endpoint connected to the private interconnect in your virtual data centre.

Traffic that passes through your secure IPsec VPN tunnel, between the two endpoints, is described as *secured traffic*.

Each IPsec VPN allows connection to one virtual data centre. You can create up to ten IPsec VPN tunnels for each virtual data centre.

Specify one or more source subnets at a single source site and multiple destination subnets in your private network – all within a single network tunnel.

Use firewall rules within your private network to restrict access to selected virtual servers.
CREATE AN IPSEC VPN TUNNEL

You can request IPsec VPN tunnels from the Connections page in the Cloud Services management console.

Name your tunnel so that it’s unique to your network and easily identifiable.

Enter the public IP address of your source endpoint.

SPECIFY YOUR SECURED TRAFFIC

Enter at least one source subnet for your secured traffic.

To specify more than one subnet on your source network, use the +add another source subnet link to add a subnet. IP subnets from the same LAN will all be contained within a single IPsec VPN tunnel.

Select a destination subnet. Multiple destination subnets can be chosen.

If you want to load balance your IPsec VPN secured traffic, you need to enter the IP address of an existing load balancer in your private network.

To access virtual servers connected to your public network through an IPsec VPN tunnel, you’ll need to connect your virtual servers to the private network as a second connection.

If you have a private firewall, you’ll need to configure firewall rules to allow IPsec VPN secured traffic. You can also use firewall rules to allow or deny traffic to and from individual servers within your private IP subnet.

Overlapping Telstra Next IP® networks and IPsec VPN tunnel source subnets can cause service disruption. None of your source IP subnets connecting to your cloud solution should overlap. It’s your responsibility to manage your IP subnets and avoid conflicts.

CONFIGURE YOUR IPSEC VPN SECURITY

Select a phase 1 security algorithm from the dropdown list.

Select a phase 2 security algorithm from the dropdown list.

Recommended options for both phases are marked. Check your local routing device to ensure it’s compatible with the security options you selected.
You choose the encryption and authentication protocols that secure your IPsec VPN connection, from the following options.

<table>
<thead>
<tr>
<th>IPSEC VPN SECURITY PHASE</th>
<th>ALGORITHM OPTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phase 1</td>
<td>AES/SHA/DH2</td>
</tr>
<tr>
<td>Lifetime: 86,400 seconds (24 hours)</td>
<td>AES/SHA/DH5</td>
</tr>
<tr>
<td></td>
<td>AES-256/SHA/DH2</td>
</tr>
<tr>
<td></td>
<td>AES-256/SHA/DH5</td>
</tr>
<tr>
<td></td>
<td>AES/MD5/DH2</td>
</tr>
<tr>
<td></td>
<td>3DES/SHA/DH2</td>
</tr>
<tr>
<td></td>
<td>3DES/MD5/DH2</td>
</tr>
</tbody>
</table>

| Phase 2                  | AES/SHA           |
| Lifetime: between 3,600 and 43,200 seconds (regardless of whether or not PFS is selected) | AES-256/SHA       |
|                         | AES/MD5           |
|                         | 3DES/SHA          |
|                         | 3DES/MD5          |

| Phase 2 perfect forwarding secrecy (PFS) | Not required |
|                                         | DH2 (1024 bits) |
|                                         | DH5 (1536 bits) |

**SUBMIT THE REQUEST**

Please take note of your pre-shared key. You’ll need to configure your local router with all the IPsec VPN settings you enter as part of the request. You can view all your settings apart from your pre-shared key, at any time in the Networks section.

**MODIFY AN IPSEC VPN TUNNEL**

Your existing IPsec VPN tunnels will be listed on the Connections page in the Cloud Services management console.

Select the tunnel you want to modify and select the Edit button.

**REMOVE AN IPSEC VPN TUNNEL**

Your existing IPsec VPN tunnels will be listed on the Connections page in the Cloud Services management console.

Select the tunnel you want to remove and select the Remove link.
CHAPTER 10
VLAN EXTENSION

Create a hybrid cloud by extending VLANs between your on-premises infrastructure and our virtual data centre, sharing an IP subnet across both environments.

Connection is through a point-to-point VLAN Extension tunnel, over your Telstra Next IP® network.

VLAN Extension can extend subnets between Telstra cloud infrastructure and any site connected to your Telstra Next IP® network, including third-party data centres or co-location facilities.

Our VLAN Extension add-on lets you extend a subnet in one of two directions:

- From your on-premises infrastructure into your Telstra cloud infrastructure private network
- From your Telstra cloud infrastructure private network, into your on-premises infrastructure

First hop redundancy protocols such as HSRP (Hot Standby Router Protocol), VRRP (Virtual Router Redundancy Protocol) and GLBP (Gateway Load Balancing Protocol) across the Telstra Next IP® network are not supported by our VLAN Extension add-on.
VLAN Extension may be configured in either a redundant or non-redundant design. Redundancy of the communication connection is achieved by supporting the VLAN Extension tunnel with an identical second compatible terminating device at your on-premises end of the tunnel.

**REQUIREMENTS TO USE VLAN EXTENSION**

To use our VLAN Extension add-on you’ll need:

- A Telstra cloud infrastructure virtual data centre in Australia
- A Telstra Next IP® network connection
- Any Telstra cloud infrastructure compute service
  - Virtual server (shared)
  - Virtual server (dedicated)
  - Managed virtual server (dedicated)
- A terminating device compatible with our VLAN Extension service
  - Cisco CSR 1000V AppX Bundle
  - Cisco Nexus 3172 (compatible IOS available from late January 2015)

For further information:

- View the CSR 1000V overview and release notes
- View the Nexus 3172 datasheet and release notes

VLAN Extension cannot be used to connect two Telstra virtual data centres. Our VLAN Extension service is not available to Telstra Global account holders.

To accommodate VXLAN protocol encapsulation overhead, ensure your terminating device and any other inpath devices in your on-premises infrastructure have an MTU size of at least 1600 bytes. Telstra managed devices are not set to 1600 bytes by default. If you have Telstra managed devices you’ll need to raise an FNC request (Feature Network Change) to increase the MTU.

VLAN Extension enables you to progressively relocate servers across a shared subnet. See our requirements and instructions for **relocating a virtual server** using VLAN Extension.
ACTIVATE VLAN EXTENSION

Once your on-premises network infrastructure has been set to at least 1600 bytes MTU, carry out the following steps to activate your VLAN Extension service:

- **Step 1 – Purchase or download a compatible terminating device**
- **Step 2 – Request VLAN Extension**
- **Step 3 – Set up the device**

**STEP 1 - PURCHASE OR DOWNLOAD A COMPATIBLE TERMINATING DEVICE**

Devices can be purchased through your Telstra representative or a Cisco reseller. We sell, but do not manage this type of device as part of our VLAN Extension service. Devices which have been tested and identified as compatible include:

- Cisco CSR 1000V AppX Bundle
- Cisco Nexus 3172 (compatible IOS available from late January 2015)

You can test the Cisco CSR 1000V virtual appliance option by downloading a free trial version and purchasing a licence key at a later date through a Cisco reseller.

The CSR 1000V is available in several licence-based speed options. For greater speeds the Nexus 3172 (N3K-C3172PQ-10GE) physical device may be preferred. Your maximum achievable speed will also be limited by your infrastructure and network access service.

**ONGOING SUPPORT FOR YOUR DEVICE**

Hardware and software support for both the Cisco CSR 1000V and Cisco Nexus 3172 can be purchased through your Telstra representative or Cisco reseller.

We recommend purchasing Cisco Technical Support when purchasing your device. This support will provide access to the [Cisco Technical Assistance Centre](#) via phone or online.

In addition, Cisco support forums may help to answer your technical questions.

**IF CHOOSING THE CSR 1000V DEVICE**

To enable all the service features of VLAN Extension you’ll require a free evaluation licence or a commercial purchased licence for the Cisco CSR 1000V AppX Bundle

Your licence must be activated before configuring your device.

**DOWNLOAD THE CSR 1000V**

To download the Cisco CSR 1000V you’ll need to create a Cisco.com (CCO) username.

Go to [https://tools.cisco.com/RPF/register/register.do](https://tools.cisco.com/RPF/register/register.do) then complete the required fields and submit. Note your password as this will not be emailed back to you.

You’ll receive an email from Cisco. Select the link in this email to activate your account.

Confirmation of your account activation will be displayed, and you’ll receive a second email from Cisco verifying the username you entered on the registration form.
If downloading version 3.13 or above, follow instructions provided through www.cisco.com.

After your username is verified, you’ll receive an email from Cisco containing a link. Select this link and enter your Cisco username and password you successfully registered previously.

The Cisco file exchange will load in your browser. From the options displayed, select the image for your Cloud Service Router and accept the terms and conditions at the bottom of the page. The Telstra special image will download.

Once download is complete, you’re ready to request our VLAN Extension service.

**STEP 2 - REQUEST VLAN EXTENSION**

After completing step 1, go to the Connections page in the Cloud Services management console.

To create a new tunnel, select *Add VLAN Extension tunnel*.

Complete the request form and submit your request.

Provide your tunnel with a meaningful name – up to 20 characters in length including letters, numbers, hyphens, spaces and underscores.

You’ll need to assign each of your tunnel endpoints with a /32 loopback address. The loopback addresses must come from new /32 subnets you assign from your private address space, outside of the subnets you’re extending. Make sure that you advertise the on-premises tunnel endpoint IP address to your Telstra Next IP® network via your on-premises router. Refer to the *Advertising IP addresses* section later in this chapter.
Now you can choose to extend a subnet from either your on-premises infrastructure or from Telstra’s cloud infrastructure. Before you do this, make sure you read and understand the section on *Gateway Location*.

The subnet address shown below is an example only. The description may display differently to indicate the status of your request.

![Extend subnets]

Select your compute service and enter your IP subnet, ensuring it doesn’t overlap with any subnets already configured in the same virtual data centre.
The addresses in this diagram are provided as an example.

**ADVERTISING IP ADDRESSES**

Make sure that you advertise the on-premises tunnel endpoint IP address to your Telstra Next IP® network via your on-premises router. You can submit a request to advertise IP addresses via the Online Feature Network Changes (Telstra FNC) website as part of Telstra Order Online. You also have the option of utilising the service desk to request the FNC change at an additional cost. Telstra FNC is accessed online via the Your Telstra Tools portal or the Managed Data Networks Support Desk on 1800 815 851.

**GATEWAY LOCATION**

For each extended subnet, traffic flow is determined by the location of your gateway. It’s through the gateway that traffic from other sites on your Telstra Next IP® network is routed to your extended subnet – either our cloud platform or your on-premises router.

If you’re extending a subnet from cloud infrastructure into your on-premises infrastructure, your gateway will initially remain in our virtual data centre. At this stage the extended subnet will continue to be advertised by our cloud platform to your Telstra Next IP® network. To redirect traffic bound for the extended subnet to your on-premises router, you must request the subnet be advertised out of your local Telstra Next IP® network service via the Cloud Services management console Connections page. If you request to extend an existing subnet from your on-premises infrastructure into our cloud infrastructure, your gateway will initially remain in your on-premises environment.

If you want to extend a subnet from your on-premises infrastructure, and have the gateway located in our virtual data centre, you’ll need to do this in two stages:

- First, add the subnet to your private network through the Network & security page in the Cloud Services management console
- Wait until your new subnet is active before extending it via a VLAN Extension request

Whenever the gateway for an extended VLAN is located in our virtual data centre we require the first three useable IP addresses of the extended subnet for configuration. This is not needed if the gateway of the VLAN remains in your on-premises environment. You may need to re-allocate IP addresses for any on-premises virtual servers or devices using the first three available IP addresses of an extended subnet. To avoid service disruption, you'll need to do this before requesting your gateway location in our cloud infrastructure.

You can choose to **change the location of your gateway** after your subnet is extended.

**NETWORK CONFIGURATION**

To allow communication between your on-premises virtual servers and cloud infrastructure virtual servers you may need to allow traffic through your on-premises private firewall.

A firewall within your private network in Telstra cloud infrastructure controls traffic between:

- **Inside-to-inside** – communication between virtual servers protected by the firewall within the cloud infrastructure private network
- **Inside-to-outside** – communication from virtual servers protected by the firewall to IP addresses outside the firewall including on-premises servers on extended subnets

For performance reasons, we recommend that any network resources (such as load balancers) you’d like to apply to your extended subnet, are configured in the same location as your gateway.

Only virtual servers in your cloud infrastructure private network are directly accessible via VLAN Extension. You can access virtual servers in your public network by connecting them to your extended private subnet as a second connection (dual homing).

Make sure all of your on-premises equipment (routers, switches or firewalls in the traffic path) have been configured to an MTU of at least 1600 bytes.

**STEP 3 - SET UP THE DEVICE**

Make your terminating device(s) accessible to your Telstra Next IP® network. You’ll require a second device for a redundant solution. You’ll have to make sure your VTEP (tunnel end-point) /32 loopback address has been advertised to your Telstra Next IP® network.

Depending on your network design, you may need to create firewall rules to allow communication between VTEP IP endpoints on UDP port 4789. Both VTEP endpoints are specified by you, and entered in your VLAN Extension service request form (step 2).

A unique VXLAN Network Identifier ID (VNI ID) was automatically generated for each extended subnet when you submitted the request. Your VNI ID(s) will need to be configured on your device, as well as other variables.
Cisco provides generic instructions on how to set up the device(s). You may find these Cisco configuration guides useful:

- **Configuration guide for Cisco CSR 1000V**
- **Configuration guide for Cisco Nexus 3172**

For specific set up instructions relating to VLAN Extension, refer to our **CSR device configuration** later in this guide.

We’ll configure the cloud infrastructure endpoint of the tunnel, and notify you when it’s ready to use.

Once your service is activated, you can change your gateway location if required.

You are now ready to **relocate servers** or create a hybrid cloud environment.

**CHANGE THE GATEWAY LOCATION**

Changing gateway location may disrupt access to your servers, and require configuration by both you and Telstra. Your service will be disrupted during a gateway change if your IP subnet is routed to both your on-premises infrastructure and cloud infrastructure environment.

Whenever the gateway for an extended subnet is located in our virtual data centre we require the first three available IP addresses of that subnet for configuration purposes. This is not required if the gateway of the extended subnet remains in your on-premises environment. You many need to re-allocate IP addresses for any on-premises virtual servers or devices using the first three available IP addresses of an extended subnet.

To minimise your service downtime, you should aim to configure your on-premises device, during or as close to the time window when we configure our cloud infrastructure.

To request a gateway change, go to the **Connections** page in the Cloud Services management console.

Select **Modify tunnel** and choose the extended subnet you want to modify.

You have the option of requesting either a:

- **Gateway change** – we’ll configure our cloud infrastructure at a time selected by us, between 1PM and 8PM (AEST), up to three business days from time of request
- **Scheduled gateway change** – you nominate a preferred and alternative date and time window when we’ll carry out our cloud infrastructure configuration

Submit your request.

**MODIFY AN ENDPOINT IP ADDRESS**

Your existing VLAN Extension tunnels will be listed on the **Connections** page in the Cloud Services management console. Both endpoints (VTEPs) of each VLAN Extension tunnel are shown.

Select **Modify tunnel** to access the tunnel configuration page, where you can modify your tunnel IP addresses.

If changing the IP address of an on-premises tunnel endpoint, ensure the new IP address is advertised correctly and reachable on your Telstra Next IP® network.

If changing the IP address of a Telstra cloud infrastructure tunnel endpoint, we’ll advertise your Telstra Next IP® network to this address.
RELOCATE A VIRTUAL SERVER

VLAN Extension enables you to progressively relocate servers across a shared subnet. It also allows you to migrate a server in a compatible format (e.g. OVF) to or from a virtual server (dedicated) service in cloud infrastructure. Note that VMware vMotion cannot be used for this purpose.

To import server data into our cloud infrastructure, it must be in a format of OVA or OVF to be recognised by the ESXi host in our VMware environment.

A virtual server can be exported from a virtual server (dedicated) service in either OVA or OVF format. To import a virtual server into your on-premises environment, ensure your destination virtualisation platform is compatible with either OVA or OVF data formats.

To migrate packaged servers and data between environments, we recommend the following steps:

- Power-off the virtual server you wish to migrate
- Export your server in either OVA or OVF format
- Use the management connection to access your destination virtualisation platform such as vCenter
- Import your server and data through your destination virtualisation platform. If maintaining the same IP address of your virtual server, ensure there are no address conflicts in your destination environment.

To transition an on-premises server to a virtual server (shared) or managed virtual server (dedicated) compute service in cloud infrastructure, recreate the server in its new infrastructure environment. If you wish to relocate the IP address with it, be sure to shut down the server in its original location, before initiating your new virtual server.

DISCONNECT AN EXTENDED IP SUBNET

Your extended subnets will be listed on the Connections page in the Cloud Services management console.

To disconnect a subnet, expand the VLAN Extension section and identify the tunnel that contains the subnet, then select Modify tunnel.

Select the subnet you want to disconnect and select the Disconnect subnet link.

REMOVE A VLAN EXTENSION TUNNEL

Your existing VLAN Extension tunnels will be listed on the Connections page in the Cloud Services management console.

You can’t remove a tunnel until all its subnets have been removed first.

To remove a VLAN Extension tunnel, expand the VLAN Extension section and next to the tunnel you want to remove, select the Remove link.
A dual homed virtual server has both a public and private IP address, allowing it to be accessed through both your public and private network connections.

This creates a number of possible connection combinations. You could access a dual homed virtual server via:

- The internet and a Telstra Next IP® network
- The internet and an IPsec VPN tunnel
- The internet and a Telstra Next IP® network and an IPsec VPN tunnel

Telstra Next IP® network is only available to access Australian data centres. International data centre users have an equivalent Global IP VPN network connection.

Dual homing can also be used to allow communication between virtual servers contained in different networks (public and private).

**ADDING A SECOND NETWORK CONNECTION TO A VIRTUAL SERVER**

You can connect a virtual server to multiple networks in any order – create your private connection first, and add a public connection at any time, or vice versa.

If you initially chose to connect your virtual server to a private network, you can add a second connection to your public network using a public IP address. This may incur a public IP address fee.

If you initially created your virtual server with a public network connection, you can add a second connection to your private network using a private IP address.

The process for doing this will vary depending on the virtual server type.

A virtual server (shared) can have a second network connection added through the Cloud Services management console.

For a virtual server (dedicated), add a second network connection through vCenter. All private IP addresses on virtual servers (dedicated) are managed by you. Public IP addresses need to be requested through the Cloud Services management console.

A managed virtual server (dedicated) can have a second network connection added through the Cloud Services management console.

**VIEWING A VIRTUAL SERVER’S SECOND NETWORK CONNECTION**

In the Cloud Services management console, click the Modify connections button in the Network tab of a virtual server.

You can view the details of all your virtual server’s network connections.

The original network connection can’t be removed.
LOAD BALANCING IN YOUR SECOND NETWORK

You may already have a load balancer configured for your virtual servers in their original network. To load balance the traffic in your second network you’ll need to configure a separate load balancer for the second network.

FIREWALLS IN YOUR SECOND NETWORK

Your virtual servers may already have firewall rules configured in their original network. To restrict traffic through your second network connection, you’ll need to configure separate firewall rules in the second network.

DIRECTING PRIVATE TRAFFIC WITH STATIC ROUTING

To complete the set up of a second network connection to a virtual server, you’ll need to configure the static routing in your virtual server’s operating system. This ensures your server’s outbound traffic is sent through the appropriate network connection.

Once manually configured, static routing will send private traffic (destined for any private IP address) through your virtual server’s private network connection. All traffic destined for a public IP address will be sent through your virtual server’s public network connection.

If you have an office LAN connected to an IPsec VPN tunnel using a public IP subnet as a secured traffic source subnet, and you are connecting to either virtual server (shared) or virtual server (dedicated) virtual server types, then you’ll need to configure routes toward this subnet using your private network vNIC.

Managed virtual servers (dedicated) won’t require any routing configuration by you – we’ll take care of this for you.

The way to configure static routing varies depending on your virtual server’s operating system. See the appendix in this user guide for details.
CHAPTER 12
FIREWALLS

You can create firewalls in both your public and private networks to increase the security and privacy of your virtual servers.

Neither private networks or public networks are created with default firewall rules – all network traffic is allowed until a firewall is created. For your data security, we recommend firewall rules are configured in your public network before any virtual servers are created.

Security policies can be created independently of IP addressing, including by reference only to virtual server names.

Firewalls can be used to group and separate virtual servers into zones and tiers and control traffic through your public and private interconnect to your virtual servers. To see examples of this, refer to our *Infrastructure Design Guide*.

A single firewall can control traffic for a single compute service, within a single network, within a single virtual data centre. You can add firewalls as you need them for each of your compute services, networks and data centres.

To configure firewall rules you’ll need to specify the source and destination of traffic, as being located either *inside* or *outside* a specific firewall.

*Inside* includes only the virtual servers directly protected by a firewall.

*Outside* includes traffic from your public or private interconnect, and other virtual servers in the same network that may be protected by another firewall.

One of these locations must be your nominated traffic source, and the other your traffic destination. This choice only applies to the particular firewall you’re configuring rules for.
You can add firewall rules for the following traffic flows:

- Outside-to-inside - communication from network(s) outside the firewall to virtual servers protected by the firewall
- Inside-to-outside - communication from virtual servers directly protected by the firewall to network(s) outside the firewall
- Inside-to-inside - communication between servers under the same virtual data centre service

You’ll need to configure firewall rules on both firewalls to allow communication between virtual servers protected by different firewalls, in the same network. Configure outside-to-inside and inside-to-outside rules on both firewalls.

If you’re dual homing a virtual server, you may already have firewall rules configured in their original network. To restrict traffic through your second network connection, you’ll need to configure separate firewall rules in the second network.

When you add a firewall you can create **allow** and **deny** rules. All traffic that does not match the allow rules will be blocked. For details of firewall fees, see the **Pricing Guide** for your virtual data centre location.

**ACCESSING THE FIREWALLS SECTION**

You can access the Firewalls page of the management console under the **Network & security** section.

**ABOUT THE FIREWALLS SECTION**

From the firewalls page, you can:

- **Add firewall**
- **Add firewall rules**
- **Edit firewall rules**
- **Re-order firewall rules**
- **Remove firewall rules**
- **Remove a firewall**
ADDING A FIREWALL

Choose one of your existing virtual data centres you would like to add a firewall to. A firewall can only control traffic for a single virtual server type within a network, within one virtual data centre. You can use the network diagram displayed on screen to select a firewall.

ADDING A FIREWALL ON VIRTUAL SERVER (SHARED)

From the options that appear, to begin with, select the firewall rules closest to your requirements. When you select one of the firewall rules options, its details are displayed. You can then either:

- Go ahead and create your firewall using these rules
- Use these firewall rules as a starting point for configuring your firewall

Read how to configure your firewall rules in the next section. When you’re happy with your firewall rules configuration, click the Add firewall button. This is an automated process for virtual server (shared) which will be completed in just a few minutes.

ADDING A FIREWALL ON VIRTUAL SERVER (DEDICATED) AND MANAGED VIRTUAL SERVER (DEDICATED)

Creating a firewall on these virtual server types is a manual process, meaning it will take up to three business days for us to complete your request.

Once created, a firewall will initially allow all traffic by default. You can modify the firewall as soon as it becomes active. Modifying an active firewall is an automated process, completed in a matter of minutes.

CONFIGURING A FIREWALL

Locate the firewall you want to configure. Use the search bar if you need help finding an existing firewall rule.

You can confirm your active firewall rules by clicking View active rules.
## ADDING A FIREWALL RULE

Configure firewall rules by specifying:

- Action to allow or deny traffic
- Source
- Destination
- Inside and outside locations
- Ports and protocols

When configuring the firewall's source and destination, you'll need to specify the inside/outside locations. You can choose to allow/deny all or select specific IP addresses. You can specify specific IP addresses by IP address, IP range or IP subnet text field.

For virtual servers (shared) you can create virtual server-to-server rules by selecting individual virtual servers by name.

When configuring ports and protocols you can choose to allow/deny all or select specific ports and protocols.
The available options are:

<table>
<thead>
<tr>
<th>PROTOCOL</th>
<th>PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP AND/OR UDP</td>
<td>Any port or port range</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
</tr>
<tr>
<td>TFTP</td>
<td>69</td>
</tr>
<tr>
<td>RSH</td>
<td>514</td>
</tr>
<tr>
<td>ICMP</td>
<td>Not applicable</td>
</tr>
</tbody>
</table>

It is possible to change the pre-populated port numbers for FTP, TFTP and RSH.

If you select FTP, TFTP, or RSH the firewall will be configured to perform deep packet inspection and allow access on ports that are dynamically negotiated.

Remember to submit your changes once you’ve finished configuring you rules.

**EDITING FIREWALL RULES**

To launch the *Edit firewall rule* window, select *Edit* next to the firewall rule you would like to modify.

Change the details in the fields you would like to modify and then *Add rule to request*.

The modified rules will be highlighted blue in the firewall rules table.

You’ll need to select *Apply changes* for the rule edit to take effect.

**RE-ORDERING FIREWALL RULES**

Note: it takes 3-5 minutes to complete this request.

Select *Edit* for the firewall rule you want to reorder.

If no other changes are needed apart from reordering, select *Add rule to request*.

Drag the firewall rule to the desired position.

Select *Apply changes*.

**REMOVING FIREWALL RULES**

Select *Remove* next to the firewall rule you would like to delete.

You’ll need to select *Apply changes* for the rule edit to take effect.
REMOVING A FIREWALL

Go to the firewall page in the Cloud Services management console.

Select the firewall you would like to remove and select Remove.

REMOVING A FIREWALL ON VIRTUAL SERVERS (SHARED)

On virtual servers (shared), removing a firewall is an automated process that only takes a few moments.

To temporarily allow traffic through a firewall, you could modify rules to allow all traffic rather than removing the firewall altogether. By doing this you’ll avoid the set-up fee that may be charged for reinstating a firewall.

To allow all traffic you’ll need to set the following temporary rules:

<table>
<thead>
<tr>
<th>ACTION</th>
<th>SOURCE</th>
<th>DESTINATION</th>
<th>PORT AND PROTOCOL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Outside: all</td>
<td>Inside: all</td>
<td>Any</td>
</tr>
<tr>
<td>Allow</td>
<td>Inside: all</td>
<td>Outside: all</td>
<td>Any</td>
</tr>
<tr>
<td>Allow</td>
<td>Inside: all</td>
<td>Inside: all</td>
<td>Any</td>
</tr>
</tbody>
</table>

REMOVING A FIREWALL ON VIRTUAL SERVERS (DEDICATED) AND MANAGED VIRTUAL SERVERS (DEDICATED)

For these types of virtual servers, removing a firewall is a manual process that can take up to three business days.

You may want to modify the firewall to allow all traffic before submitting the request to remove the firewall. Modifying an active firewall is an automated process that takes only a few moments to complete.
CHAPTER 13
LOAD BALANCERS

Add load balancers to your network to distribute traffic to multiple virtual servers. A single load balancer can service a combination of server types (shared, dedicated and managed dedicated) within a network.

CREATE A NEW LOAD BALANCER

You can request load balancers from the Load balancers page in the Network & security section of the Cloud Services management console.

You’ll need to choose which network the load balancer should be created in.

If you choose a public load balancer, we’ll allocate a public IP address to the load balancer.

If you choose a private load balancer, you’ll need to provide an IP address. This IP address can’t come from any IP subnets that you have allocated to your private network.

Please provide a name for the load balancer application you’d like to set up.

Select the application protocol type from the dropdown menu.

The virtual IP port and server port numbers will be automatically entered depending on the application protocol type you selected. You can also change these numbers.

If you select other from the Application protocol type dropdown, another dropdown will appear to give you the option to specify the transport protocol (TCP or UDP). You’ll need to enter the Virtual IP port and server port numbers yourself.

Specify which virtual server(s) will be included in the load balancing pool.

SELECT THE LOAD BALANCING METHOD

The methods include:

Least connections: Directs traffic to the virtual server with the least number of current connections.

Round robin: Directs traffic to each virtual server in sequence.

Hash: Assigns traffic based on the source IP address. Hash uses persistent connections to the same server, so can be used when standard persistence methods (below) are not applicable (e.g. non-HTTP traffic or if you require persistence longer than sticky source IP’s 24 hours). This method can produce uneven distribution.

If you selected either Least connections or Round robin as your load balancing method, you can choose to add a persistence option. If you choose None, traffic will be directed according to the specified load balancing method.

Persistence options offers ways to send traffic to the same virtual server.

Sticky source IP: Maintains stickiness using the source IP address, but only for 24 hours.

Persistent cookie: Maintains stickiness using a cookie stored in the user’s browser. When you choose this method, you can then select to have the cookie time-out up to one year.
**Session cookie:** Identifies traffic using a cookie, but only for a browser session.

You will only be able to select the *Persistent cookie* and *Session cookie* options if you specified your application protocol as HTTP.

**HEALTH MONITORING**

Health monitoring helps a load balancer determine which virtual servers are and aren't available. Select the health monitoring method you would like to use:

*Ping:* A Ping health check sends an ICMP echo request packet to the server and awaits an echo response. If you have configured a firewall, your virtual server may not respond to pings unless you allow it and may be incorrectly labelled as ‘down’ as a result.

*TCP/UDP (socket open):* A TCP/UDP (socket open) health check does a basic check of the server port (e.g. TCP port 80) to see if a virtual server will accept a connection.

*HTTP any code:* A HTTP any code health check initiates a HTTP request to the virtual server and waits a response of any code. The virtual server will be marked as *up* as long as the HTTP server can reply to the request (including if it replies with error codes such as 404). If you want to use the root URI, enter ‘/’.

*HTTP OK code:* A HTTP OK code health check is similar to HTTP any code, but only marks the server as ‘up’ if it receives HTTP codes of 200, 201 or 202. If you want to use the root URI, enter ‘/’.

Supported load balancer port and protocol configurations are limited to the options provided through the Cloud Services management console. Available options are:

<table>
<thead>
<tr>
<th>APPLICATION PROTOCOL</th>
<th>VIP PORT</th>
<th>SERVER PORT</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>80</td>
<td>80</td>
</tr>
<tr>
<td>HTTPS</td>
<td>443</td>
<td>443</td>
</tr>
<tr>
<td>FTP</td>
<td>21</td>
<td>21</td>
</tr>
<tr>
<td>DNS</td>
<td>53</td>
<td>53</td>
</tr>
<tr>
<td>SMTP</td>
<td>25</td>
<td>25</td>
</tr>
<tr>
<td>SSMTP</td>
<td>465</td>
<td>465</td>
</tr>
<tr>
<td>IMAP</td>
<td>143</td>
<td>143</td>
</tr>
<tr>
<td>IMAP4-SSL</td>
<td>993</td>
<td>993</td>
</tr>
<tr>
<td>IMAPS</td>
<td>585</td>
<td>585</td>
</tr>
<tr>
<td>POP3</td>
<td>110</td>
<td>110</td>
</tr>
<tr>
<td>POP3-SSL</td>
<td>995</td>
<td>995</td>
</tr>
<tr>
<td>OTHER (TCP OR UDP)</td>
<td>User specified</td>
<td>User specified</td>
</tr>
</tbody>
</table>

A load balancer performs a health check every 15 seconds.

A virtual server will be marked as *down* if it fails a health check three times in a row (45 seconds). Once marked down, a virtual server will be removed from the load balancing pool and no new traffic will be sent to it.

Existing connections to a failed server will need to *time out* before it can reconnect to the load balancer and reach a new virtual server.
Once marked as *down*, a virtual server will continue to be health checked every 60 seconds. It will be marked as *up* if it passes three health checks in a row (180 seconds). Once marked as up, it will be re-added to the load balancing pool.

**MODIFY AN EXISTING LOAD BALANCER**

Your existing load balancers will be listed on the *Load Balancers* page in the Cloud Services management console.

Select the load balancer you want to modify and select the *Modify this load balancer* link. Then you only need to enter the load balancer details you would like to change and submit the request.

**REMOVE AN EXISTING LOAD BALANCER**

Select the load balancer you want to modify and select the *Remove* link.

**ACCESS YOUR CONFIGURATION DETAILS**

Can’t remember the configuration details of your load balancer? Select the load balancer you want to modify and select the *Request current configuration* link. The configuration details will be emailed to you.
There are several methods for remotely managing individual virtual servers of any type, located in any network. In addition to a public and private vNIC, all virtual servers have a third potential connection point - a management vNIC reserved for management and backup purposes only. This connection can’t be used as a secure access point for end users.

Management communication with your virtual servers takes place via the internet.

There are a number of third-party software options that will allow you to establish a management connection with a virtual server. Several of the connection methods our protocols support, are:

- A secure remote access (SSL VPN) connection (recommended)
- An unsecured remote desktop or SSH connection

Instructions for establishing these connection options appear below.

**SSL VPN MANAGEMENT CONNECTION TO VIRTUAL SERVERS**

SSL VPN communicates through a secure client-to-site network tunnel, used to remotely access virtual servers from the internet over HTTPS. SSL VPN connects directly to a virtual server’s management vNIC.

You can access the SSL authentication page through a web browser. Once authenticated, the security appliance offers access to the SSL VPN client. After downloading, the client will install and configure itself and establish a secure SSL connection.

All network traffic will be transmitted using a secure network connect tunnel configured with split tunnelling that ensures only traffic destined for the virtual server is routed through the tunnel. All other traffic will be routed through your default network route.

To access your virtual server, you’ll need:

- Your virtual server’s management IP address
- Access to either Remote Desktop software or a Linux secure shell client

Each virtual data centre location you wish to manage, will require a separate SSL VPN connection.

You can use management connection’s secure IP address to RDP or SSH to the virtual server. You can find the management area via the virtual server’s Network tab in the Cloud Services management console.

**CONNECT USING REMOTE DESKTOP SOFTWARE**

You can connect to a virtual server running Windows using Remote Desktop software.

Enter your server’s IP address and then click Connect.

You will then be prompted to provide your server’s login details.
CONNECT USING A SECURE SHELL CLIENT

You can connect to a virtual server running Linux using a secure shell client, such as Putty.

Enter your server’s IP address, make sure that SSH is selected, and click Open.

You will then be prompted to provide your server’s login details.

You’ll be able to log into the Cloud Services SSL VPN login page after you’ve set up the first SSL VPN user. The login page address will vary depending on your virtual data centre location:

- Australia
  - Melbourne: https://vic.access.cloud.telstra.com
  - Sydney: https://nsw.access.cloud.telstra.com
  - Perth: https://wa.access.cloud.telstra.com
- Singapore: https://sg.access.cloud.telstra.com
- Hong Kong: https://hk.access.cloud.telstra.com
- London: https://uk.access.cloud.telstra.com

You can’t add a SSL VPN user until you have a virtual server up-and-running. It will take up to three business days to set up a SSL VPN connection.

MANAGING SSL VPN USERS

You can manage SSL VPN users from the Management SSL VPN page in the Network & security section of the Cloud Services management console.

From the SSL VPN section, you can:

- Create SSL VPN users
- Modify existing SSL VPN users and reset passwords
- Remove existing SSL VPN users

CREATE SSL VPN USERS

You’ll need to have a virtual server set up before you can create a SSL VPN user.

Enter the new SSL VPN user’s details and submit the request.

We’ll email you a username and a temporary password for the new user(s).

The new user will need to log into the Cloud Services SSL VPN login page to update the password.

You can create as many SSL VPN users as you need.

You need to create SSL VPN users for each of your virtual data centres.
MODIFY SSL VPN USERS

1. Select the Modify tab.
2. Enter the full name, username or email address to identify the user whose details you would like to modify. Only fill in the details you would like to change.
3. To reset a SSL VPN user’s password, select the Reset password checkbox and submit the request. We’ll email you a temporary password.

REMOVE EXISTING SSL VPN USERS

1. Select the Remove tab.
2. Enter the full name, username or email address to identify the user who you would like to remove.

ACCESS YOUR CONFIGURATION DETAILS

Can’t remember your configuration details? Send a request to have your configuration details emailed to you.
CHAPTER 15
SMTP MAIL RELAY

All outbound email traffic originating from mail servers operating within the cloud must be sent through our SMTP mail relay service, or alternative software we can provide.

For the full list of SMTP mail relay fees, see the Pricing Guide for your virtual data centre location.

ACCESS THE SMTP MAIL RELAY SECTION
Access the SMTP mail relay section via the Network & Security Management section.

From the SMTP mail relay details page, you can:

- Request an SMTP mail relay
- Remove an SMTP mail relay

REQUEST AN SMTP MAIL RELAY

You’ll need to provide one or more valid outgoing email domain names.

After you submit the request to add an SMTP mail relay, we email the mail server set-up details to you.

You’ll then need to configure your software accordingly.

All emails sent via SMTP mail relay must use one of the domain names you specified in the set up process, in the from field of the email. Using any other domain name will cause the email to be rejected.

REMOVE AN SMTP MAIL RELAY

To stop using our SMTP mail relay service, remove the SMTP mail relay server settings from your virtual servers.

You will no longer be able to send emails from your virtual servers.

ALTERNATIVES TO SMTP MAIL RELAY

We allow the use of several software alternatives to using our SMTP mail relay service.

Microsoft® Office 365, Symantec.Cloud and internet protection (email) can be provided and supported through Telstra. For details, click on the names of the software products in the following table.
The following software and outbound port connectivity is permitted:

<table>
<thead>
<tr>
<th>SOFTWARE</th>
<th>PORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Microsoft® Office 365</em></td>
<td>25, 465, 587</td>
</tr>
<tr>
<td><em>Symantec.cloud</em></td>
<td>25</td>
</tr>
<tr>
<td><em>Internet protection (email)</em></td>
<td>25</td>
</tr>
</tbody>
</table>
The following information will help you manually route private and internet traffic, when a second network connection is added to a virtual server. The instructions vary based on the operating system of the virtual server.

For your virtual server to send traffic to your private network, you'll need to configure static routes on your private network connection for the following private IP subnets:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

Use the first IP address of your private IP subnet as the gateway address.

**STATIC ROUTING VIRTUAL SERVERS RUNNING WINDOWS**

Any virtual server with a second network connection, running any version of a Windows based operating system, will need three routes to be added:

Route -p add 10.0.0.0 mask 255.0.0.0 <private gateway>
Route -p add 172.16.0.0 mask 255.240.0.0 <private gateway>
Route -p add 192.168.0.0 mask 255.255.0.0 <private gateway>

If you have an office LAN connected to an IPsec VPN tunnel using a public IP subnet as a secured traffic source subnet, configure routes toward this subnet using your private network vNIC.

Route -p add <IPsec public source subnet> mask <IPsec mask> <private gateway>

The <private gateway> field refers to the first IP address of the private network subnet your virtual server is connected to. So for example, if your virtual server’s private network subnet is 10.1.0.0/23, then 10.1.0.1 is the private gateway.

**STATIC ROUTING VIRTUAL SERVERS RUNNING LINUX**

Any virtual server with a second network connection, running any version of a Linux based operating system, will need three routes to be added:

10.0.0.0 mask 255.0.0.0 <private gateway>
172.16.0.0 mask 255.240.0.0 <private gateway>
192.168.0.0 mask 255.255.0.0 <private gateway>

The <private gateway> field refers to the first IP address of the private network subnet your virtual server is connected to. For example, if your virtual server’s private network subnet is 10.1.0.0/23, then 10.1.0.1 is the private gateway.

The next steps required will vary depending on the version of Linux your virtual servers are using.
REDHAT, ORACLE OR CENTOS LINUX OPERATING SYSTEMS - EXAMPLE CONFIGURATION FOR ONE ROUTE

1. Apply the static routes to the vNIC connected to your private network. The following instructions assume eth2 for this configuration (adapt this to your specific vNIC).

2. Static routes should be configured in `/etc/sysconfig/network-scripts/route-eth2` using the following format:

   - 10.0.0.0/8 via <private gateway>
   - 172.16.0.0/12 via <private gateway>
   - 192.168.0.0/16 via <private gateway>

3. If you have an office LAN connected to an IPsec VPN tunnel using a public IP subnet as a secured traffic source subnet, add an additional route to the same file `/etc/sysconfig/network-scripts/route-eth2`

   - <IPsec public source subnet> via <private gateway>

4. To apply the previously defined static routes, you'll need to restart the network services using the following command:

   ```
   # service network restart
   ```

SUSE LINUX OPERATING SYSTEM - EXAMPLE CONFIGURATION FOR ONE ROUTE

1. Apply the static routes to the vNIC connected to your private network. The following instructions assume eth2 for this configuration (adapt this to your specific vNIC).

2. Static routes should be configured in `/etc/sysconfig/network/ifroute-eth2` using the following format:

   - 10.0.0.0/8 <private gateway> - eth2
   - 172.16.0.0/12 <private gateway> - eth2
   - 192.168.0.0/16 <private gateway> - eth2

3. If you have an office LAN connected to an IPsec VPN tunnel using a public IP subnet as a secured traffic source subnet, add an additional route to the same file `/etc/sysconfig/network/ifroute-eth2`

   - <IPsec public source subnet> <private gateway> - eth2

4. To apply the previously defined static routes, you'll need to restart the network services using the following command:

   ```
   # /etc/init.d/network restart
   ```
CHAPTER 17
APPENDIX B: VLAN EXTENSION CSR DEVICE CONFIGURATION
1. `vlan_ext_srv_vlan`
2. `vlan_ext_local_ip`
3. `vlan_ext_remote_ip`

Refer to table below for a full list of commands and descriptions

You’ll need to configure your on-premises Cisco CSR 1000V terminating device(s) to enable a VLAN Extension service. The following configuration templates relate to step 3 – set up your device as part of the VLAN Extension activation instructions.

If you are using a VMware vSphere Standard Switch to connect the CSR 1000V device, the port group will need to allow for promiscuousness.

The following device configuration instructions assume:

- **GigabitEthernet1** is the WAN interface connected to your Telstra Next IP® network
- **GigabitEthernet2** is the VLAN trunk interface carrying VLANs to be extended
The command instructions include variables listed in the table below:

<table>
<thead>
<tr>
<th>VARIABLE COMMAND</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_ext_srv_vlan</td>
<td>on-premises VLAN to be extended</td>
</tr>
<tr>
<td>vlan_ext_vni</td>
<td>VXLAN Network Identifier (VNI)</td>
</tr>
<tr>
<td>vlan_ext_local_ip</td>
<td>on-premises VTEP IP address</td>
</tr>
<tr>
<td>vlan_ext_remote_ip</td>
<td>cloud infrastructure VTEP IP address</td>
</tr>
<tr>
<td>vlan_ext_HSRP_IP1</td>
<td>primary CPE physical interface IP address</td>
</tr>
<tr>
<td>vlan_ext_HSRP_IP2</td>
<td>secondary CPE physical interface IP address</td>
</tr>
<tr>
<td>vlan_ext_HSRP_vIP</td>
<td>HSRP virtual IP address</td>
</tr>
<tr>
<td>vlan_ext_WAN_sub_mask</td>
<td>WAN IP subnet mask</td>
</tr>
<tr>
<td>vlan_ext_gw_IP</td>
<td>WAN gateway IP</td>
</tr>
</tbody>
</table>

We provide routing device redundancy in our cloud infrastructure. Redundancy at your on-premises end of the tunnel is achieved with an identical second compatible terminating device.

To implement a non-redundant design, apply only the primary device instructions below.

To implement a redundant design refer to the separate instructions for your primary and secondary devices.

**PRIMARY DEVICE**

On your primary (or only) CSR 1000V device, enter the following commands to activate your device premium trial licence and reload the device to enable VLAN Extension features.

```
license boot level premium
wr mem
reload
```

If applicable, follow the relevant instructions in your Cisco product manual to activate your commercial licence.

Once the appropriate licence has been activated, proceed with the following configuration.

```
bridge-domain <vlan_ext_srv_vlan>
member vni <vlan_ext_vni>
member GigabitEthernet1 service-instance <vlan_ext_srv_vlan>
```
interface Loopback100
description *** On-premises VTEP IP ***
ip address <vlan_ext_local_ip> 255.255.255.255
!
interface nve1
description *** VXLAN tunnel ***
no ip address
member vni <vlan_ext_vni>
ingress-replication <vlan_ext_remote_ip>
!
source-interface Loopback100
!
interface GigabitEthernet1
description *** WAN ****
ip address <vlan_ext_HSRP_IP1> <vlan_ext_WAN_sub_mask>
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 VLAN_Extension
standby 100 ip <vlan_ext_HSRP_vIP>
standby 100 priority 130
standby 100 preempt
standby 100 authentication md5 key-string VLAN_Extension
ip ospf bfd
bfd interval 50 min_rx 50 multiplier 3
!
interface GigabitEthernet2
description *** VLAN Extension L2 services ***
no ip address
negotation auto
service instance <vlan_ext_srv_vlan> ethernet
  encapsulation dot1q <vlan_ext_srv_vlan>
```
rewrite ingress tag pop 1 symmetric
!
interface GigabitEthernet3
description *** Unused ***
shutdown
!
router ospf 1
router-id <vlan_ext_HSRP_IP1>
network <vlan_ext_HSRP_IP1> 0.0.0.0 area 0
!
ip route 0.0.0.0 0.0.0.0 <vlan_ext_gw_IP>
!
This completes your primary device configuration.

SECONDARY DEVICE
On your optional secondary CSR 1000V device, enter the following commands to activate your device premium trial licence and reload the device to enable VLAN Extension features. If applicable, follow the relevant instructions in your Cisco product manual to activate your commercial licence.

license boot level premium
wr mem
reload

Once the appropriate licence has been activated, proceed with the following configuration. Note that the Loopback100 and GigabitEthernet2 interfaces are intentionally shutdown.

bridge-domain <vlan_ext_srv_vlan>
  member vni <vlan_ext_vni>
  member GigabitEthernet2 service-instance <vlan_ext_srv_vlan>
!
interface Loopback100
description *** Customer-side VTEP IP ***
ip address <vlan_ext_local_ip> 255.255.255.255
shutdown
```
interface nve1

description *** VXLAN Tunnel ***

no ip address

member vni <vlan_ext_vni>

ingress-replication <vlan_ext_remote_ip>

!

source-interface Loopback100

!

interface GigabitEthernet1

description *** WAN ****

ip address <vlan_ext_HSRP_IP2> <vlan_ext_WAN_sub_mask>

ip ospf authentication message-digest

ip ospf message-digest-key 1 md5 VLAN_Extension

standby 100 ip <vlan_ext_HSRP_vIP>

standby 100 priority 125

standby 100 preempt

standby 100 authentication md5 key-string VLAN_Extension

ip ospf bfd

bfd interval 50 min_rx 50 multiplier 3

!

interface GigabitEthernet2

description *** VLAN Extension L2 services ***

no ip address

negotiation auto

shutdown

service instance <vlan_ext_srv_vlan> ethernet

encapsulation dot1q <vlan_ext_srv_vlan>

rewrite ingress tag pop 1 symmetric

!
interface GigabitEthernet3
  description *** Unused ***
  shutdown
!
router ospf 1
  router-id <vlan_ext_HSRP_IP2>
  network <vlan_ext_HSRP_IP2> 0.0.0.0 area 0

ip route 0.0.0.0 0.0.0.0 <vlan_ext_gw_IP>
!
event manager environment _L2sideInt GigabitEthernet2
  event manager environment _NoTouch_Interfaces
!
event manager applet WatchBFDdown
  description "Monitors BFD status, if it goes down, bring Loopback interfaces up"
  event syslog pattern "BFD node down" period 1
!
  action 1.01 set intfs ""
  action 1.02 set final_intfs ""
!
  action 2.01 cli command "en"
  action 2.02 cli command "show ip interface brief | inc Loopback"
!
  action 3.01 foreach line "$_cli_result" "\n"
  action 3.02 regexp "(Loopback[0-9]+) ." "$_line" junk intf
  action 3.03 if $_regexp_result eq "1"
  action 3.04 set intfs "$intfs $intf"
  action 3.05 end
  action 3.06 end

action 4.01 syslog msg "Potential Loopback interfaces to no shutdown: $intfs"

!

action 5.01 foreach line "$intfs"
  action 5.02 set nak "0"

action 5.03 foreach denied "$_NoTouch_Interfaces"
  action 5.04 if $denied eq "$line"
  action 5.05 set nak "1"
  action 5.06 end
  action 5.07 end
  action 5.08 if $nak eq "0"
  action 5.09 set final_intfs "$final_intfs $line"
  action 5.10 end
  action 5.11 end

!

action 6.01 string trim "$final_intfs"
  action 6.02 set final_intfs "$string_result"
  action 6.03 syslog msg "Final Loopback interfaces to no shutdown: $final_intfs"

!

action 7.01 cli command "config t"
  action 7.02 foreach line "$final_intfs"
  action 7.03 cli command "interface $line"
  action 7.04 cli command "no shutdown"
  action 7.05 end

action 7.06 cli command "interface $_L2sideInt"
  action 7.07 cli command "no shutdown"

!

action 8.00 syslog msg "EEM WatchBFDdown COMPLETE ..."

!

event manager applet WatchBFDup
  description "Monitors OSPF status, if it goes up, bring Loopback interfaces down"
event syslog pattern "\OSPF-5-ADJCHG.*from LOADING to FULL" period 1
action 1.01 set intfs ""
action 1.02 set final_intfs ""

! action 2.01 cli command "en"
action 2.02 cli command "show ip interface brief | inc Loopback"
!
action 3.01 foreach line "$_cli_result" "\n"
action 3.02 regexp "(Loopback[0-9]+) .*" "$line" junk intf
action 3.03 if $_regexp_result eq "1"
action 3.04 set intfs "$intfs $intf"
action 3.05 end
action 3.06 end
!
action 4.01 syslog msg "Potential Loopback interfaces to shutdown: $intfs"
!
action 5.01 foreach line "$intfs"
action 5.02 set nak "0"
action 5.03 foreach denied "$_NoTouch_Interfaces"
action 5.04 if $denied eq "$line"
action 5.05 set nak "1"
action 5.06 end
action 5.07 end
action 5.08 if $nak eq "0"
action 5.09 set final_intfs "$final_intfs $line"
action 5.10 end
action 5.11 end
!
action 6.01 string trim "$final_intfs"
action 6.02 set final_intfs "$_string_result"
action 6.03 syslog msg "Final Loopback interfaces to no shutdown: $final_intfs"

!

action 7.01 cli command "config t"

action 7.02 foreach line "$final_intfs"

action 7.03 cli command "interface $line"

action 7.04 cli command "shutdown"

action 7.05 end

action 7.06 cli command "interface $_L2sideInt"

action 7.07 cli command "shutdown"

!

action 8.00 syslog msg "EEM WatchBFDup COMPLETE ..."

!

This completes your secondary device configuration.