e2e assure

e2e Secure Cloud Web Gateway Service - Service Definition Document

OVERVIEW

A cloud based web browsing solution and cloud access broker that provides secure web access for users and devices. The service has three service levels that provide differing service levels (SLA's) and functionality, these can be 'mixed and matched' (users and devices can have different service levels).

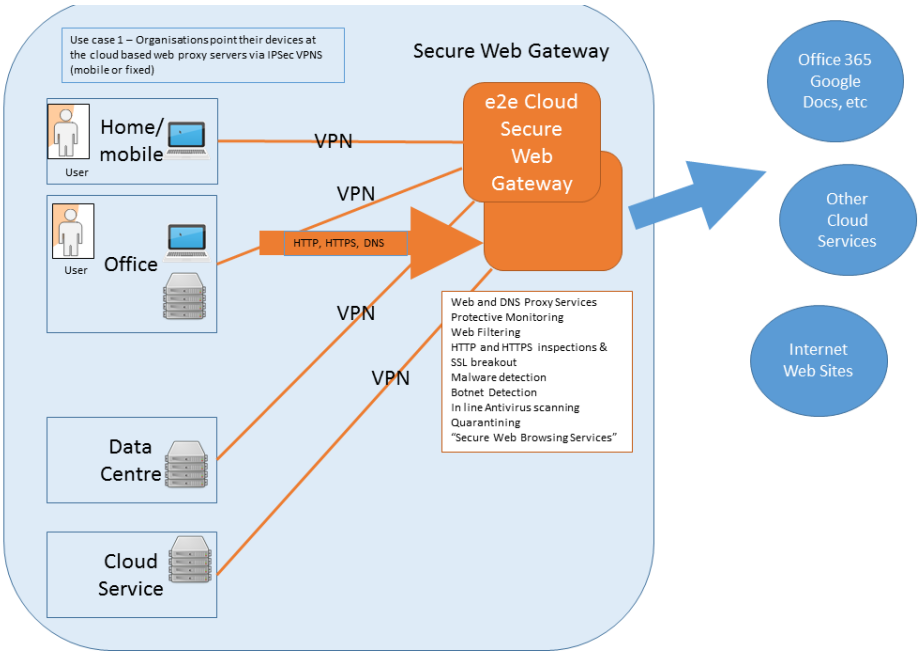
There are three main components of the service:

SECURE WEB GATEWAY

This delivers a cloud based resilient web proxy solution that provides:

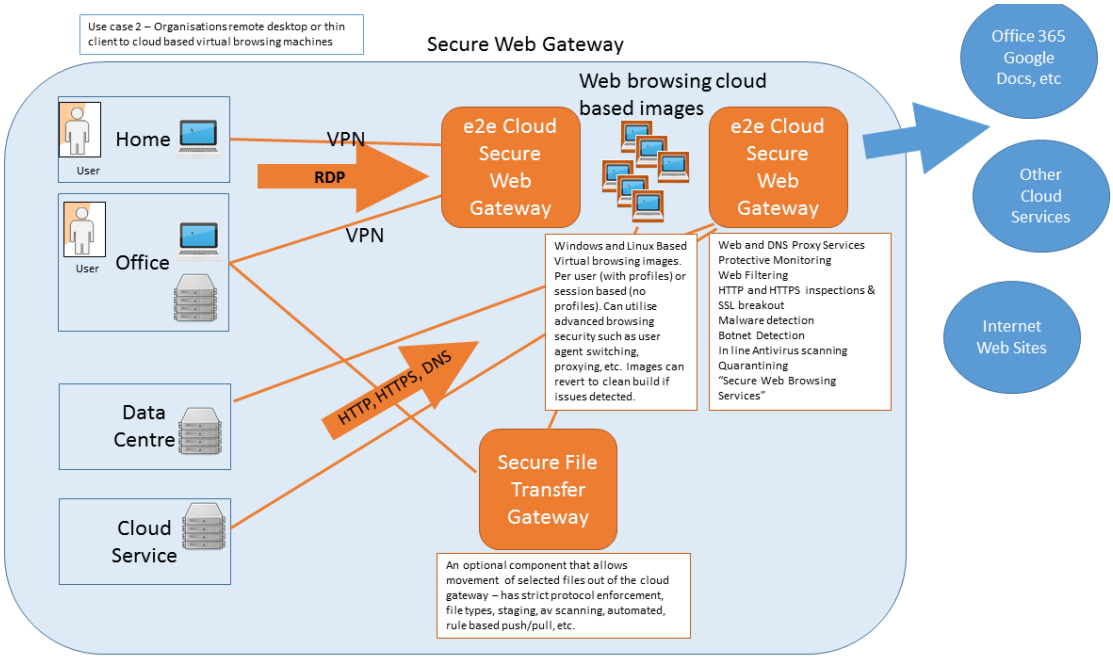
- URL filtering against predefined and customizable categories
- Content Filtering, blocking unwanted keywords and attachments, including file types, mime types and renamed files
- Content filtering based on web site scoring
- Granular controls to allow restriction polices based on user, group, IP address, location, subnet, time, OU
- SSL/HTTPS Inspection
- Anti-virus, Anti-malware and Anti-phishing blocking
- Enforce You Tube Education
- Enforce Safe Search
- Ability to whitelist at user/group/URL/OU/AD Computer name or IP level
- Ability to whitelist for a specified duration
- Ability to monitor, monitor/advise/allow and monitor/block content
- Content aware social media controls
- Comprehensive reporting providing graphical interpretations
- Ability to generate additional custom reports
- Ability to schedule report for export to email, Excel and PDF formats
- LDAP, RADIUS, ADFS, Active Directory Integration
- Full audit trail and all logs kept for between 3 months and 5 years
- Proxy services for http, https, DNS and NTP traffic
- Explicit and Transparent proxy options

The users and devices connect to the cloud based service through IPSec VPNs or through dedicated WAN connections. One significant advantage of the service is that it can be used to lock down access to other cloud services (i.e. ensure only sessions from the secure web gateway can access other cloud services).



SECURE WEB CLOUD BASED BROWSING IMAGES / VIRTUAL DESKTOPS

Delivers a browsing 'break out' solution by providing a complete desktop browsing service in the cloud; users connect to specially designed secure browsing virtual machines/images and browse from these – using thin client connectivity such as remote desktop. This is the most secure way of browsing that eliminates back channels to the organisation and provides advanced anonymity and obfuscation services such as user agent masquerading as well as other techniques to minimise the risk of web based threats.



Secure File Transfer Gateway

This component is optional and provides the ability for users or devices to transfer data from the secure web gateway. This is typically required alongside option 2 where complete segregation is being provided between users and the internet and there are use cases that require data such as screenshots and downloaded files to be securely transferred. This components of the gateway provides a host of secure file transfer services that ensures strict enforcement of rules regarding what can and cannot be transferred. It is an automated mechanism with customisable rules.

Organisations can choose a service that suits their security and service requirements. The service support Windows, Mac, Linux, most tablets, and phones and provide secure Internet access from anywhere as well as secure access to other cloud services. This is a cloud independent service which provides web filtering and secure web proxy services that deliver high levels of security as well provide necessary compliance, alerting and reporting requirements. It is a pay monthly, per user or device service that can flex up and down along with your business needs.

Features

- Managed web browsing and connection to internet
- Secure endpoint connection over internet
- Accredited Pattern: existing deployments with referenced government clients
- Web Filtering
- Active Directory integration
- http and https web filtering
- Advanced malware and threat protection from Web 2.0 threats
- Detailed reporting down to a per user view of browsing
- Flexible Deployment
- Integration into existing networks
- Web Content Filtering
- Reporting
- Administration
- Security
- E-Safety
- Compliance

Benefits

- ✓ Manage user's internet browsing and report on usage
- ✓ Maintain existing services and deploy at OFFICIAL SENSITIVE
- ✓ Future-proof against new IA guidance
- ✓ Reduce risks of malware, web threats, and other web risks
- ✓ Improve productivity by restricted access to business related web sites.
- ✓ Reduce risks of inappropriate web sites being accessed
- ✓ Automated daily, weekly, monthly reporting
- ✓ Down to the user policies and reporting
- ✓ Assign multiple administrators granularly
- ✓ Compliance

- ✓ Available as VMware or Hyper-V. Deployed Transparently or proxy
- ✓ Fully integrates with AD or other LDAP compliant structures.
- ✓ Keeps internet users browsing safe and appropriate
- ✓ Provides comprehensive audit of user access
- ✓ Includes AV, Anti -Phishing and Anti Spyware modules
- ✓ Delegated administration structure allows multi-tiered management
- ✓ Supports any device, managed or otherwise
- ✓ Protects students/users from the dangers of the web
- ✓ Protects organisations from liability issues.
- ✓ Anonymous internet access

CLOUD BASED, CLOUD FRIENDLY VIRTUAL SECURITY PERIMETER

Our Service enables you to quickly secure your organisations perimeter as well as securing your web browsing traffic. You will need to configure all your services to point to a cluster of proxy services in e2e's cloud services and close down all other outbound internet access from your other services other than these Fixed VPNs. We provision these proxy services per customer providing segregation of customer traffic as it passes through the service. This dramatically increases your security and simplifies your cloud landscape. If required we can also provide SSL inspection of all outgoing HTTPS traffic to look for threats buried in encrypted traffic. This method of cloud security is highly effective at bringing your gateway or cloud services under control and allows us to identify anomalous traffic by its characteristics as well as by matching against known threats.

Traffic reaching our service passes through one or more different security services which include:

Web proxy service

- Web filtering – Examines web traffic and blocks unauthorised content
- Web proxy – Protects your organisation by using our web proxy to examine application requests for anomalous behaviour
- Web category blocking – Protects your organisation and personnel from inappropriate web sites
- Web policy enforcement – Monitors and Enforces corporate web usage policies
- Web blacklist blocking – Prevents sites known to carry threats from being accessed or from communicating with your corporate resources
- Web whitelisting - Restricts corporate access to a known list of authorised web sites
- Web traffic antivirus – Monitors all corporate web traffic for internet borne malware
- DNS proxy – Protects against DNS attacks by using our secure DNS proxy services
- DNS filtering – Filters DNS requests to prevent Botnet or other internet attacks compromising your organisation
- NTP service – Uses our NTP service to protect against amplification DDOS attacks launched on NTP servers which can disrupt or disable business services
- Botnet Detection – Uses our service to detect and prevent Botnet subversion
- Premium Services also include Data Loss Prevention (DLP) and APT Detection

SSL Inspection Service

- SSL inspection – Uses our service to look for threats buried in encrypted traffic

Additional Protective Monitoring services

- Trojan prevention – uses our service to prevent internet borne Trojans entering your organisation
- Web traffic IPS – implements web intrusion protection to monitor and secure your corporate web traffic from threats within web packet streams
- Web traffic logging – Logs web traffic to support forensic investigations and to provide enhanced situational awareness for improved anomaly detection
- Web packet logging – Captures web traffic to support forensic security analysis and better incident response
- DNS inspection – Inspects DNS requests to gain insight into the behaviour of corporate resources to ensure that external communications are understood and follow expected patterns of use

Our gateway service has been designed by CESG CCP Senior Security Architects and assessed by CLAS consultants. Our services are CES+ Certified and ISO27001:2013 Certified, located in secure UK datacentres, and are operated using ISO27001:2013 certificated processes. All our staff are UK based and hold SC clearance as a minimum. This means that our gateway service can support your legal and regulatory compliance obligations, support your assurance requirements for connectivity to other government services and can immediately enhance your protective monitoring

HOW DO I KNOW WHICH SERVICE LEVEL IS APPROPRIATE?

There is a level of service appropriate for all organisations. If you do not currently know what the right level of service is we offer a simple process:

1. e2e provide a free, one day on site cloud workshop led by a CESG Senior IA Architect where we work with your organisation to establish your requirements and cover aspects such as your organisations risk profile and security assurance requirements, connectivity requirements as well as your platform and application requirements.

2. The workshop report includes expert advice from e2e and includes generating your heat map similar to the below and this gives us a score:

Heat Map Scoring Chart												
					★							
0-3	4	5	6	7	8	9	10	11	12	13	14	15
Very Low	Low			Medium			High			Very High		

3. This score then maps to our recommended services:

Recommended Service				
Score	Basic	Enhanced	Premium	Custom
3				
4				
5				
6				
7				
8		★		
9				
10				
11				
12				
13				
14				
15				

4. If you need more help we can provide follow up workshops with no commitment from you to purchase a cloud service. We will walk you through a risk based approach that starts with your business requirements and allows you to decide which service aligns best.

SERVICE LEVELS

We offer three service levels. Customers can move up and down service levels on a monthly basis as needs change and can choose to place devices on different levels of service according to their need.

Baseline	
Target SLA/Month (during service hours)	99.50%
Service Hours	8am to 6pm Mon-Fri
Service Hours Response Time	4 hours
Emergency/out of hours 24/7 response time	8 hours
Protective Monitoring Service	Baseline
Log retention	6 months

Enhanced	
Target SLA/Month (during service hours)	99.90%
Service Hours	8am to 6pm Mon-Fri
Service Hours Response Time	2 hours
Emergency/out of hours 24/7 response time	4 hours
Protective Monitoring Service	Enhanced
Log retention	12 months

Premium	
Target SLA/Month (during service hours)	99.99%
Service Hours	24/7
Service Hours Response Time	1 hour
Protective Monitoring Service	Premium
Log retention	24 months

ROLES AND RESPONSIBILITIES

This is a fully managed service that covers the creation of the Fixed VPNs and provision of proxy and related services described in this document. Each customer solution has dedicated VPN devices at the e2e datacentre and customers are expected to use their existing VPN devices, cloud based VPN services, client devices, and so forth – we will supply configuration settings as well as all Internet bandwidth required at our end.

The service supports most operating systems and browsers that support the configuration of a proxy server. Alternately organisations can point existing proxy servers at this service or route internet bound traffic to the service - the latter option allows for transparent proxying of traffic and is supported only with the Premium service level.

The virtual web browsing solution requires the customer to use a thin client such as remote desktop or a suitable web browser to access the virtual machine.

Your organisation will be responsible for installing and configuring any clients and supporting your end users. You will need to provide details of devices that require access to the service and let us know when your users stop using the service.

We will manage all VPN devices that we provide as part of our service to you and you will be responsible for managing any of your own VPN devices used in the service or delegating management of these devices to e2e.

If your organisation lacks the capability to in/configure or support the end user devices we can assist, either with support days or through our separate e2e Managed Peripherals Service or through the e2e Secure Cloud Connect Service.

MORE INFORMATION AND CONTACT DETAILS

For more details on this service and to see the other services we offer visit

www.e2e-assure.com

Enquiries, and more information is available on request, email info@e2e-assure.com with any queries.

WHO ARE E2E?

e2e are a cloud security company with 20 years' experience of providing military grade cyber security. We provide repeatable cloud-based services to the public sector. Security depth, quality and service excellence set us apart from our competition.

OUR ORIGINS

e2e was founded by two industry experts, each holding 20 years' experience of delivering secure, end-to-end solutions. We have a history of designing secure networks for online payment systems; designing, developing and delivering cyber defence solutions; developing and starting up complete Managed Service solutions; and have built several worldwide Data Centres. Our clients over the years have covered most sectors from banking to the MoD.

OUR PEOPLE

e2e have brought together a highly experienced team of cloud experts, developers, security architects, CESG CLAS consultants, support specialists, security analysts and expert cyber security business development specialists. This core team has since been bolstered by the addition of a vibrant cloud support and cyber analyst team, recruited through channels such as the Cyber Security Challenge UK, SANS Cyber Academy and other government backed schemes to find cyber talent.

OUR WORK IN GOVERNMENT

We have earned an excellent reputation over the last three years as a trusted service provider to government and our cloud services are helping deliver key UK wide services. All our services are ISO27001:2013 accredited, CES and CES+, IASME certified, and we are the go-to organisation when a

need for cost effective, cloud based services are required that must be secure to protect UK sovereign reputation. Our services to government cover central government, local government as well as other public sector organisations.

Our Ambitions

e2e are a service company. We have a well-developed range of cloud-based services, all of which are designed to be repeatable, scalable, flexible and on-demand.

- We aim to be the best supplier: the easiest to deal with, the most reliable, and the best at delivering cloud service support and managed services. So far we have made a huge impression with our existing customers – e2e just does it better than the competition.

- We aim to be the most secure supplier, to deliver and maintain the most secure services. There is simply no other supplier on the market with our security credentials and no other supplier with the technology and team to deliver security-as-a-service at our level. We are miles ahead in this area and this is where we want to stay.

Our Methodology

We focus on applying well established skillsets and a wealth of experience to ensure highly responsive delivery without sacrificing quality. We invest in our technology and our people so that our customers can benefit from our thirst for excellence. We understand how to integrate security seamlessly into our services, giving you secure cloud based services that 'just work'.

We have fully embraced the 'As a service' model: e2e is a cloud based business, with a cloud business model, operating model, service delivery model and we deliver all our services from our cloud based operations centre.

Our Qualifications

e2e is a UK based SME Company operating exclusively from within the UK using SC cleared staff. We operate out of two UK datacentres (Tier3 and Tier4). We are ISO27001:2013 accredited, CES and CES+, IASME certified, CLAS members, CESG CCP Senior level, UKCEB members, TechUK members, BCS and IoD members, Crown Commercial Suppliers, UK Cyber Security Forum members. We sponsor and recruit from the Cyber Security Challenge UK as well as the SANS Cyber Academy. We understand how to work with partners and ensure we are honest and straightforward to deal with. We embrace the cloud first approach and are heavily involved in UK Cyber in general; we want to help spread the UK cyber messages (CESG Cloud Security Principles, 10 steps, Get safe on line, etc.) and are active CiSP members with strong links within UK Cyber.