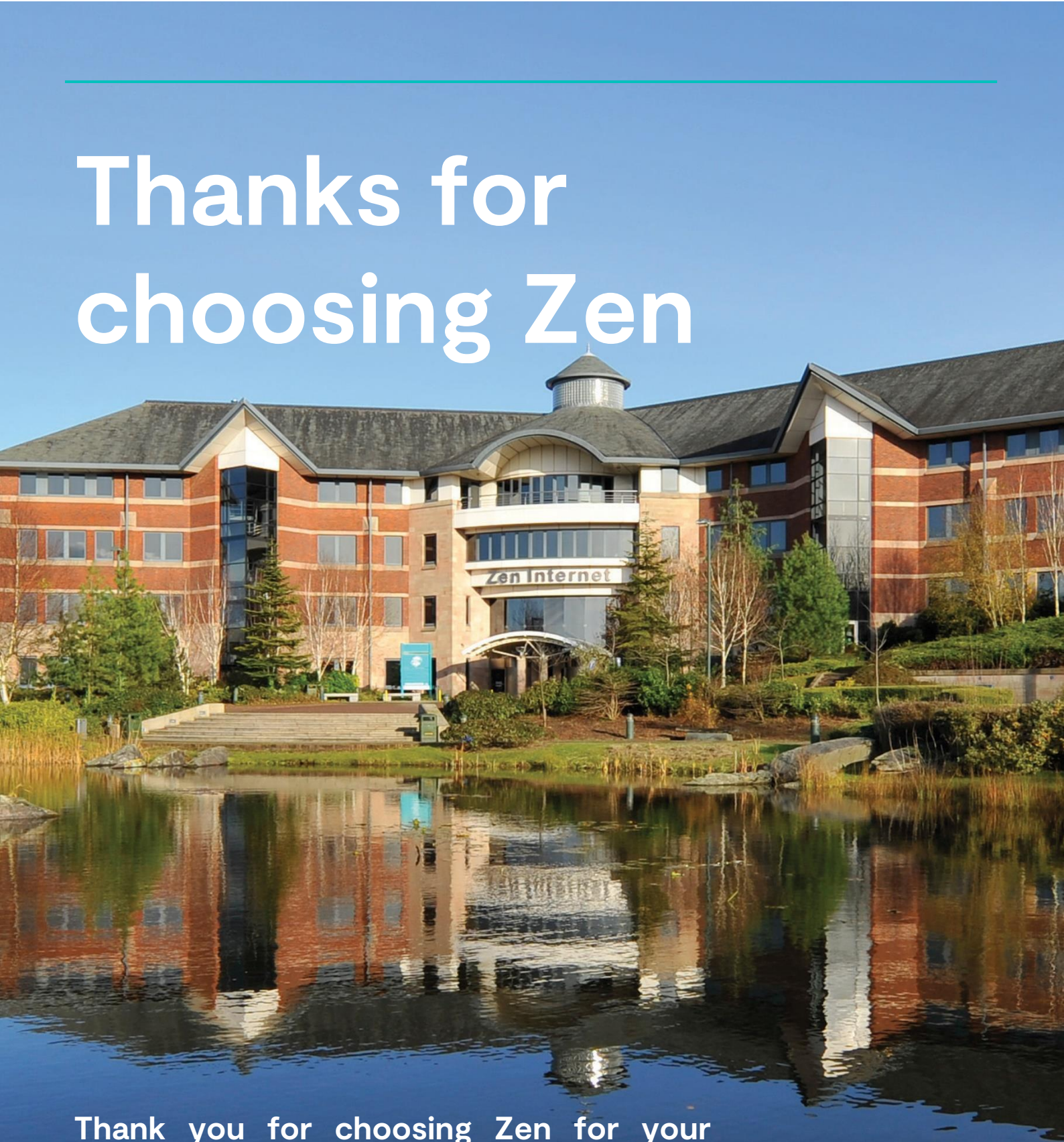
Managed Firewall Services

Customer Service Plan

Thanks for choosing Zen



Thank you for choosing Zen for your Managed Firewall. This pack provides you with all the information and guidance you need to order any new and manage your existing Firewall Services with Zen.

Ordering services & product enquiries

Service offering

Managed Firewall use cases vary in the deployment approaches taken to achieve the customer's desired business outcomes. It is important to note that within this document there may be some delivery and management difference between the key service offerings.

IPVPN solution: High Availability clusters, Network Segmentation, or Geographically Diverse Internet Breakout.

On premise network security: Perimeter security and / or secure network to network connectivity.

To order new Zen Managed Firewall services or to enquire about product specific information, availability and pricing:

Stage	Contact
Firewall Order Placement	Zen Account Manager

Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Order placement – key stages

- Requirements capture and design stage:
  A Customer Solution Architect (CSA) assigned to review and capture your requirements as part of the firewall solution design.
- Project management:
  Depending on the complexity of the solution being deployed, a Project Manager will be assigned to initiate and co-ordinate the build and deployment activities (Typically this is for core IPVPN services). Requirement for the activity to be project managed will be identified by Zen at the requirement capture stage.
- Quote generated (including project management, licencing / supporting network ports where appropriate).
- Quote accepted and Order form completed by the Customer.

Order acceptance and delivery

Data validation is completed prior to acceptance of an order. Incorrect / missing data will lead to a delay in order acceptance and service provision.

Following receipt of an order, the Zen Order Management team will process the order within 3 working days.

An order acceptance email, containing a unique order reference number will be emailed to the pre-designated customer order contact.

Service provision enquiries & updates

Stage	Contact
Complex – Typically core IPVPN deployment	Zen Account Manager / Project Manager
Non-Complex – Typically On-Premises	Zen Engineering Logistics 01706 902 650 engineering.logistics@zen.co.uk

Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Target response time for queries – 8 working hours

Firewall build

Firewall build activities will be carried out in collaboration with the customer as per solution requirements. Build times may vary depending on solution complexity.

Activity	Standard Target Lead Time
Delivery of the Managed Firewall	Typically 15 working days for a basic solution

Service installation

The Managed Firewall appliance(s) will be deployed upon completion of the requisite build activities.

On-premise install:
Where devices are not installed within a Zen Datacentre, the device will be shipped to the destination in co-ordination with the customer.

Note: It is the customer's responsibility to arrange any device shipping outside of the UK.

Device installation is the responsibility of the customer. Remote deployment support from a Zen engineer can be provided upon request.

Note: 72 hours' notice is required for any customer initiated booking request to schedule a managed install with a Zen engineer.

Zen are also able to offer a field engineering service to perform on-site deployment. Professional Service Charges may be applicable.

Stage	Contact
On-site Firewall deployment support – Professional service charges apply	POA via Zen Account Manager

Zen datacentre install:

Device installation within a Zen Datacentre will be managed by Zen. Change windows will be agreed in advance with the customer to ensure that operational disruption (if any) is kept to a minimum. Out of Hours installation can be conducted upon request and will be subject to professional service charges. Further clarification can be sought from the Zen Account Manager / Project Manager.

Stage	Contact
Core Firewall deployment - Professional service charges may apply	Zen Account Manager / Project Manager

In-life service issues
Incident management

Stage	Contact
In-life service issues	Zen Service Desk 01706 902 222 managed.support@zen.co.uk

Core business hours

Incident Priority	Incident Cover
P1 – Critical	24/7/365
P2 – High / P3 – Normal	Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays) Weekend / Bank Holidays – Closed

Proactive incident logging

Managed Firewall services are monitored and managed 24/7/365. Any monitoring alerts will be proactively managed by the Zen Service Desk team who will endeavour to contact the customer's pre-agreed in-hours / out-of-hours order specific technical contact at the earliest opportunity.

Exceptions: Firewall deployments as a terminating device e.g. IPSEC termination.

Reactive incident logging

The customer must:

- Be a Named Contact on the account and compliant with GDPR requirements.
- Be able to provide the Zen reference pertaining to the service affected by the issue.
- Provide the description of the issue being experienced and any (additional) reasonable information requested by the Service Desk.

Incident acceptance and resolution

Once a service fault has been established and to support timely resolution, the customer must provide a Named Contact who will be responsible for;

- Receiving incident updates via email or phone and sharing that internally to the affected site users,
- Owning the problem from a customer's perspective,
- Consenting to any potential charges that may be applicable,
- Providing site availability should Zen need to dispatch an Engineer to the customer's premises,
- Providing a site contact who can provide site access for supplier engineers (if required),
- Testing service post resolution,
- Confirming that service has been resumed in order for the incident to be closed.

Service SLA

Service	Target Fix Time	Incident Cover
Managed Firewall – Device Failure	Replaced by next business day (where site access is available)	24/7/365

Note:

- Target fix times for the Geo-resiliency option - secondary device is next business day + 1.
- For on-premises device failures, the replacement device will be shipped to a customer designated destination on mainland UK. It is the customer's responsibility to arrange any device shipping outside of the UK.

Service Desk prioritisation

Priority	Impact Definition	Target Initial Response Time
P1 – Critical	Total service unavailable or severe operational issue with no workaround	Within 1 working hour
P2 – High	Operational issue that results in partial service availability	Within 4 working hours
P3 – Normal	Standard changes or an operational fault where a workaround already exists so that business can continue with little or no impact	Within 8 working hours

Note:

- Fault Fix target lead-times may be subject to change where a Force Majeure is in effect.
- P1 or P2 incidents reported by customers must be followed up by a telephone call to the Zen Service Desk.

Escalation matrix
Incident management

You can escalate through the following stages using the escalation criteria specified below:

Considered response time 4 working hours CC Level 3, Level 1 & Zen Service Manager (If applicable)	Level 4	Head of Technical Support	Customer – Senior Management	Escalate via Manager
Considered response time 3 working hours CC Level 2, Level 1 & Zen Service Manager (If applicable)	Level 3	Technical Support Manager	Customer – Manager	Maintain escalation Level 3 contact Escalate to Level 4 if Escalation Criteria met at Level 3
Considered response time 2 working hours Initial acknowledgement 1 working hour CC Level 1	Level 2	Technical Support Team Leader support.escalations@zen.co.uk	Customer – Service Desk	Maintain escalation Level 2 contact Escalate to Level 3 if Escalation Criteria met at Level 2
Escalation Entry, Qualification and Acceptance Preferred method: Telephone	Level 1	Service Desk managed.support@zen.co.uk 01706 902 222	Customer – Service Desk	Escalation Request Preferred method: Telephone

Escalation Criteria:

- Poor quality of updates
- Customer is not satisfied at the way that the incident is being managed
- Agreed plan of action or timescales at a specific escalation level are not met
- The support team have not responded to an email within target response time of 8 working hours
- Frequency of updates does not meet what has been agreed with the customer

Note: Escalations can only be raised by the Customer contacts who are registered as named contacts against the Order for which the escalation is being requested on Escalations will be accepted and managed: Mon – Fri 09:00 - 17:00 (Escalations outside of these hours will be managed on a best endeavours basis)

Change management

Stage	Contact
In-life change & Information requests	Zen Service Desk 01706 902 222 managed.support@zen.co.uk

Core business hours

Monday – Friday 9:00am – 5:00pm (exc. Bank Holidays)
Weekend / Bank Holidays – Closed

Request for change / information

Any Zen Managed Firewall policy / configuration change or request for access to information must be logged via the Service Desk by either telephone or email. When making contact the customer must;

- Ensure that the requested is submitted by designated / authorised change approver on the account and compliant with GDPR requirements.

When requesting a change, the customer must provide:

- Relevant RFC document(s) to provide clear and comprehensive details of the requested change.
- The customer lead contact name(s), contact details and availability (Working hours and outside working hours if applicable) for the purposes of;
  - ✓ Authorising change implementation,
  - ✓ Authorising change window for Non-standard changes,
  - ✓ Testing and post change success validation.

When requesting access to information, the customer must provide:

- A list of information parameters required on the output information report.
- If applicable, the name of existing Managed Firewall report template containing the information parameters required.

Service Desk Change / Information Request Prioritisation

Priority	Impact Definition	Target Initial Response Times
P1 – Critical *Incident Cases Only	Emergency configuration change to resolve an incident causing estate wide total loss of service or major impact to customer business operations.	Within 1 working hour
P2 – High	Standard Changes expedited in accordance with customer urgency and impact statement. *Subject to acceptance.	Within 4 working hours
P3 – Normal	Standard Changes & Information requests.	Within 8 working hours

All requests are logged as a P3 priority as standard. Should there be a requirement to escalate the prioritisation level of the request, the Zen Service Desk will need to be contacted via telephone.

A Zen Engineer will agree appropriate request priority levels depending on customer urgency and impact statement.
Any change request work required to be completed outside of core business hours will be subject to an additional charge.

Stage	Contact
Out-of-Hours Change request application	Contact Service Desk POA via Zen Account Manager

Non-routine change requests / Service enhancements

All customer Managed Firewalls will be delivered as per the agreed initial design and are subject to customer signoff. Delivery of requests for complex additions and enhancements in-life may be subject to further design activities and professional service charges. Examples or such requests include but are not limited to:

- SSO / LDAP Integration
- Enablement of MFA
- Large scale time sensitive requests e.g. network redesign to be completed within a short timeframe

Request Category	Charge
Routine & Non-complex	N/A
Non-Routine and Complex change(s) *Requires Solution design. Professional charges apply	Contact Service Desk POA via Zen Account Manager

Managed firewall information report requests

Standard Firewall reports are provided by default and setup as part of the Firewall deployment process.

Standard Report	Reporting Period	Reporting Frequency
Threat Report	Previous 24 Hours	Daily
Bandwidth & Application Report	Previous 7 days	Weekly
Web Usage Report	Previous 7 days	Weekly
IOC Summary Report	Previous 7 days	Weekly

- Standard / Non-standard requests for information

Information Access Request Type	Request Classification	Charge	Target Lead Time
Information captured within the last 14 days	Standard	N/A	8 working hours
Information older than 14 days*	Non-standard	£75 per request	5 working days
New Scheduled Firewall Report	Non-standard	£75 per request	5 working days
Changes to Existing Report Template	Non-standard	£75 per request	5 working days
Bespoke Request	Non-standard	Contact Account Manager	
High Volume Request	Non-standard	Contact Account Manager	

*Customer log information is retained for a period of 90 days.

Solution management

Firewall auditing

Zen will provide an annual audit of the customer firewall configuration to review and ensure best practice implementation. The audit is presented as a report to the designated customer contact(s) and followed up with a consultation with a Zen Security Engineer (if applicable and deemed necessary). Any redundant configuration items identified in this process will be monitored and retired where appropriate and also include identifying and strengthening of any potential weak configuration. Any subsequent change requests that are required will be handled as per the standard change process.

Ad-Hoc audit reports can be generated upon request and will be subject to a Professional Service charge.

Firewall Audit	Charge
Annual	N/A
Ad-hoc	POA via Zen Account Manager

Customer access

Where customers have a business need to have live visibility of Firewall policies, secure read-only remote access accounts can be created and managed by the Zen Service Desk. Users requesting remote access changes should be a named contact within the Zen System for audit purposes.

Co-managed (Zen + Customer) access to the firewall can be provided on a case by case basis providing:

- Relevant training has been delivered to the customer.
- Agreement on potential risks and SLA impact obtained from the customer.

Client software version

If SSL VPN client(s) or FSSO capability has been implemented on the solution, it is the customer's responsibility to ensure that they are using the most up to date release of the software version.

Click here for SSL VPN

Click here for FSSO

Moves and maintenance

Managed firewall physical moves

In some circumstances, there may be a requirement for the physical relocation of the deployed Firewall within or between Zen Data Centre Facilities. Examples of this may be to establish geographic resilience or to secure different parts of a customer network.

Stage	Contact
Firewall relocation	Zen Account Manager / Project Manager

Managed firewall firmware upgrades

Planned maintenance: All firewalls are maintained on recommended firmware versions for vendor support and security purposes. Zen standard policy is to maintain N -1 from the latest vendor firmware version to ensure appropriate testing and validation has be conducted. Firewall upgrade notifications will be issued to the designated customer contact(s) at least 10 working days in advance of the work being scheduled.

Exceptions: Emergency Maintenance (but not limited to) resolve an incident, resolve a known error, to ensure Regulatory compliance etc.

Emergency maintenance: A firmware upgrade maybe deemed as a mandatory emergency requirement to resolve (but not limited to) vendor PSIRT advisories - https://fortiguard.com/psirt. Zen reserve the right to apply an emergency maintenance window to carry out these maintenance activities. We will endeavour to provide as much notice as possible but this may not be possible in all situations.

Zen network maintenance activities

Zen carry out regular network maintenance and on occasion this may affect the network infrastructure which supports the firewall device. Both IPVPN and On-Premise devices may be affected by Planned Maintenance activities and in all cases, Zen will use best endeavours to provide 10 working days' notice of any work which may be disruptive to the underlying firewall network connectivity.

Customer-led maintenance activities

On occasion, customers need to carry out on-site maintenance on site which may affect the availability of the firewall service (e.g. Power maintenance). It is recommended that the customer informs Zen of the maintenance at least 24 hours in advance to ensure monitoring alarms and subsequent call outs are suppressed.

Stage	Contact
On-site customer led maintenance	Zen NOC 01706 902 010 noc@zen.co.uk