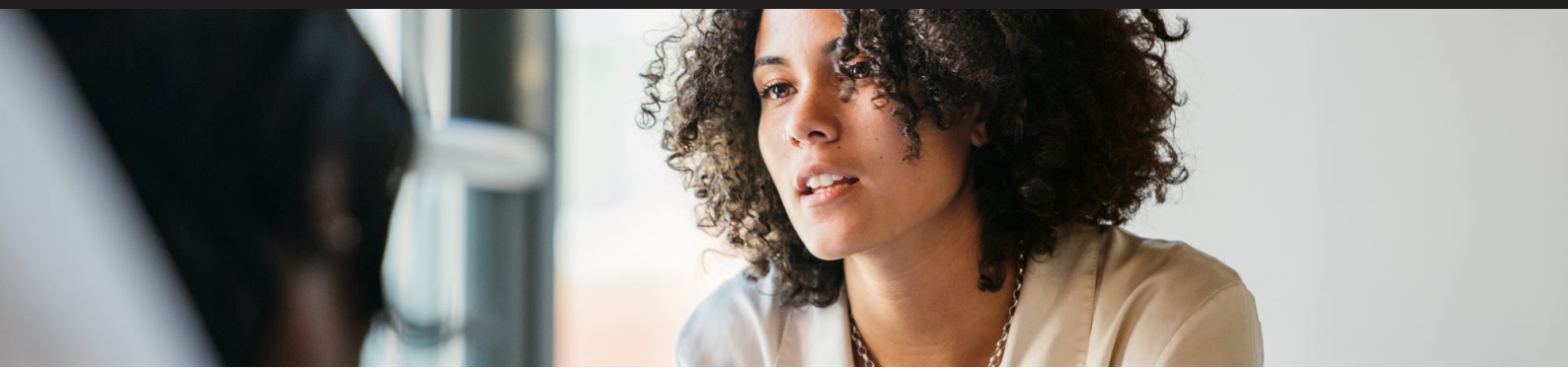
Orange
Cyberdefense



Service overview

Managed Next-Generation Firewalls

Key benefits

Enhanced security
Threat Prevention additions (Intrusion Detection/Prevention, Anti-Malware, Application Control, User Identity Awareness) assists prevention of malicious user- and application behaviour.

Reduced risk
Intercepting and blocking at the application layer prevents breaches and avoids regulatory compliance violation.

Incident alert
Identification and notification of issues related to device availability.

Proactive monitoring
Subject to contract, 24x7x365 proactive monitoring of key device metrics.

Service-desk support
Subject to contract, 24x7x365 support to remediate issues in normal operation of scoped appliances.

Patching, updates and upgrades
Where performed remotely, full deployment of patches, updates and upgrades to the device specific software.

Change assessment and management
a) In coordination with change processes and change windows specific to the customer business and, b) Assistance with the creation and implementation of risk-assessed changes.

Business continuity
Weekly backups of device policies and hardware configuration.

Service description

Considering that every company that has been breached has had firewalls in place indicates that traditional firewalls, often the first line of defence for a business, are incapable of combatting modern threats. The current dynamic threat landscape means firewalls now need to be application aware, inspect traffic content, intercept malware and offer intrusion detection/ prevention capabilities.

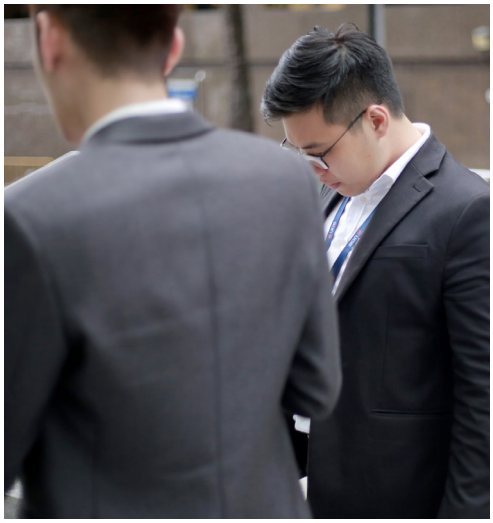
Next-generation firewalls offer the additional layers of inspection and detection required to increase an organisation's resilience to an attack. These layers may comprise of:

- Anti-Virus/Anti-Malware
- Anti-Bot
- Application Visibility and Control
- User Identity Awareness
- Intrusion Prevention
- Web URL Filtering
- Web Content Filtering

While these additional features offer significantly better protection, they do create additional burden on resource-starved IT staff and add device management complexity to ensure they remain effective and deliver return on investment.

Our fully managed Next Generation Firewall service removes the complexity of continuous rule-base management allowing in-house IT teams to focus on the tasks the business needs.

The service also increases visibility into user behaviour, network and application-layer traffic through Intrusion Detection and Prevention, extends protection against web-based attacks using Web Content and URL filtering and reduces the risk of malware infection through virus, malware and bot detection.



Why Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Orange Cyberdefense retains a 25+ year track record in information security, 250+ researchers and analysts 16 SOCs, 10 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries.

We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Key service component

Managed firewall

- Ongoing rule-base configuration mitigating against new and emerging threats
- Unlimited Site-to-Site VPN creation and configuration (device dependant)
- Site-to-Site VPN tunnel monitoring and performance-testing (subject to dedicated AffinitySECURE system being in place and device dependant)
- ISP failure monitoring for internet-facing gateways subject to access being enabled by the ISP

Managed intrusion detection and prevention

- Initial application of one baseline policy to each device followed by finer tuning for a period of 30 days working with the customer to configurepolicies according to required actions and severity
- Ongoing fine-tuning of IDS/IPS policies and signatures as requested by the customer
- Signature updates deployed according to agreed customer schedule.

Managed threat prevention

- Anti-Virus, Anti-Malware and Anti-Bot signature database updates implemented as released by the vendor
- Emergency implementation of 'hotpatch' signatures, as per agreed BAU change process
- Maintenance of Threat Prevention exclusion lists

Managed application control and identity awareness

- Policy creation and management to identify, allow, block or limit usage of social networks, applications and features within applications
- Change management of user access to company resources and Internet applications
- Custom policy creation with centralised policy management

Managed URL- and web content filtering

- IP address/domain signature database updates as released by the vendor
- Custom Proxy Auto-Config (PAC) and Whitelist/ Blacklist creation and maintenance (subject to scoping documents)
- Web content security policy and rule-base management