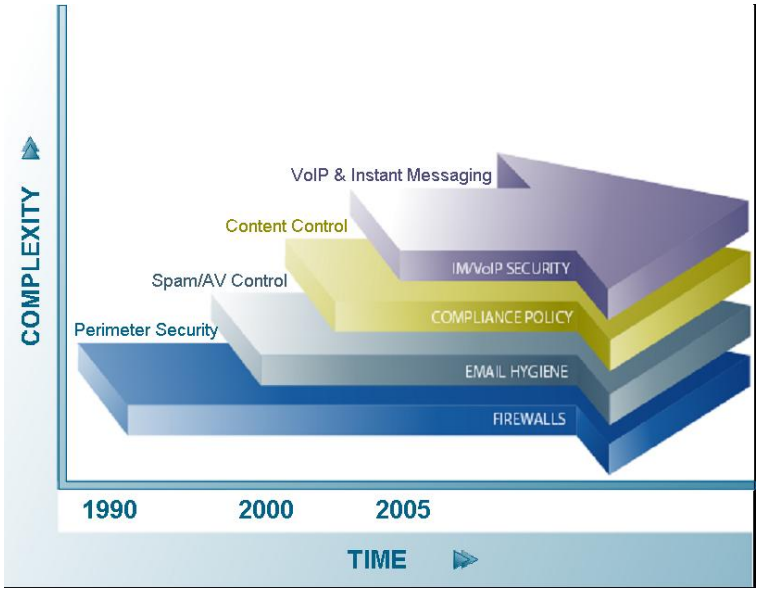
Solución de AntiSpam y Antivirus
de
WatchGuard

Sobre XCS de WatchGuard

- Empresa Canadiense fundada en 1994
- Dedicada a la fabricación de productos de seguridad:
  - **XCS eMail Firewall,** seguridad del vector email, navegación web y las comunicaciones por mesajeria instantanea.

    - AntiSpam y control del contenido de los emails.
    - Antivirus
    - Control de accesos a Internet
    - Seguridad de la mensajeria Instantanea.



- Actualmente presente en 65 países con más de 8.000 clientes.
- Un canal de distribución con mas de 500 revendedores.

- Fue el primer fabricante en adoptar la certificación EAL4+ en un cortafuegos

- XCS Email Firewall es el único appliance de seguridad de correo-e que ha obtenido la certificación EAL4+

- La actual solución de convergencia de soluciones de seguridad llamada “Integrity” permite administrar desde un solo punto y con un solo administrador, todos los servicios que ofrece el fabricante.

Como Trabaja XCS Email Firewall

XCS de WatchGuard es líder en el mercado en el apartado de las soluciones de AntiSpam. Su tecnología dispone de los recursos y la infraestructura propios para hacer una prevención de ataques en tiempo real.

Vamos a disponer de los componentes necesarios para poder prevenir los ataques, realizar un control de contenidos y herramientas de gestión de todo el entorno.

Prevención de ataques

XCS Email Firewall de XCS de WatchGuard dispone de una serie de elementos que nos van a detectar los ataques que pueden sufrir nuestros usuarios, los componentes son:

XCS Email Firewall Intercept Engine (Anti-Spam)

- Protección integrada contra spam, virus, DoS, Directory Harvest, Phishing, y ataques por inundación en tiempo real

BSN (XCS de WatchGuard Security Network)

- Servicios de reputación Local & global propios
- Protección amenazas a nivel de Conexión

Conectores Cisco y F5

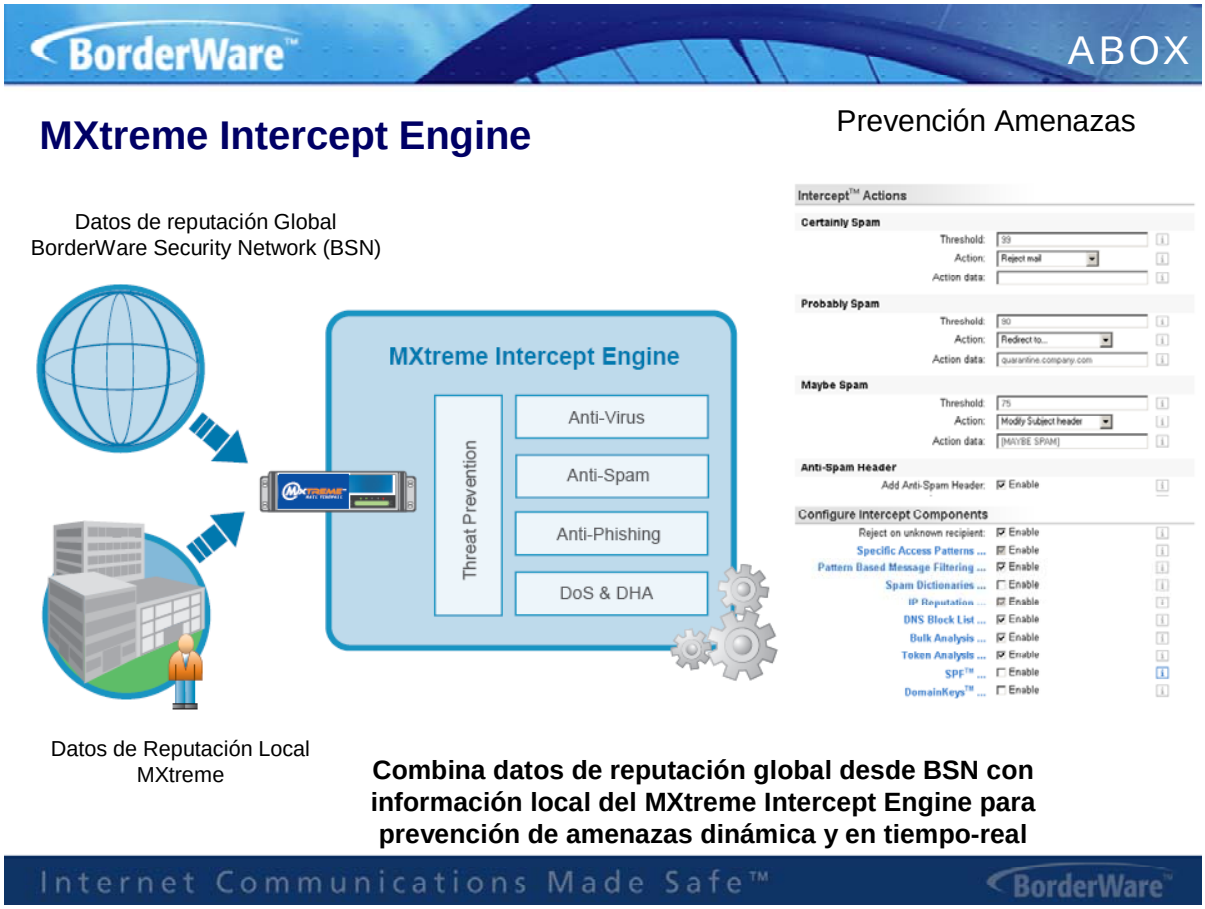
- Integración con infraestructura de red para prevención proactiva de amenazas en el perímetro de la red

Servicios de Autenticación de Remitente

- Prevención de ataques phishing utilizando DomainKey + Sender Policy Framework

Microsoft Exchange Plug-in

- Integración transparente con entornos Exchange



Principales componentes del Intercept Engine

Los principales componentes del Intercept Engine son los siguientes:

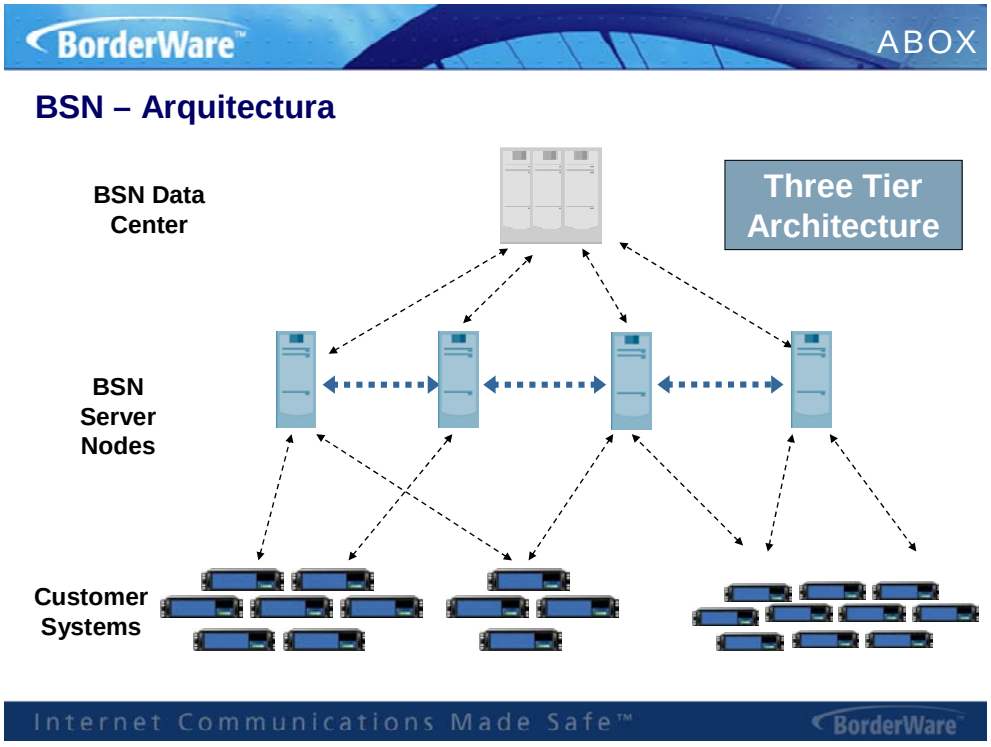
- Specific Access Pattern
- Pattern Based Messages Filtering
- Spam Dictionaries

- Mail Anomalies
- DNS Block List
- URL Block List
- Bulk Analysis
- Token Analysis & Image Spam Detection
- Sender Policy Framework (SPF)
- DomainKeys Authentication

XCS de WatchGuard Security Network

Es una red global de detección de amenazas, el fabricante aprovecha la extensa distribución de sus soluciones, de forma que los mismos clientes colaboran en la detección de amenazas, alimentando de información la red de servidores de seguridad de XCS de WatchGuard en el mundo.

- Es una red global de sistemas en la que los clientes que colaboran en el bloqueo de las amenazas de red y aplicaciones
- Recibe información de todos los participantes:
  - Información sobre fuentes de SPAM, virus, ataques directorio, ataques de denegación de servicio, etc
  - Diferentes tipos de productos (XCS Email Firewall, Firewall) proporcionan información de diferentes amenazas
  - También recoge información “buena” para proporcionar una opinión balanceada



La información de BSN puede utilizarse de dos formas:

- Para rechazar conexiones durante la sesión SMTP:
  - Remitentes maliciosos conocidos pueden ser rechazados incluso antes de recibir ningún correo-e

- En la estratégia de decisión de XCS Email Firewall Intercept:

  - Dicha información puede utilizarse para decidir si es un mensaje spam
  - Proporciona una “segunda opinión” para correos dudosos

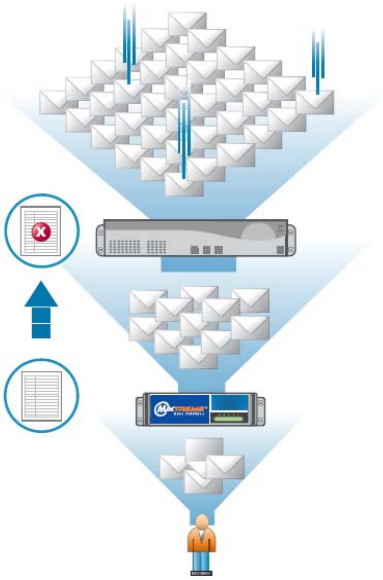
Servicios de Reputación Local & Global

Con una red propia de servidores, es capaz de mantener en tiempo real información de los ataques presentes en la red y saber desde que IP se realizan.
Esto permite disponer de :

- Detección y respuesta a amenazas en tiempo real
- Más que un servicio de reputación IP
- Paro de ataques cuando la campaña se está lanzando
- Combina datos procedentes de cortafuegos, cortafuegos de correo-e, cortafuegos SIP y appliance de red (F5 & Cisco)
- Otros servicios sólo utilizan datos del remitente de correo-e
- http://bsn.XCS de WatchGuard.com, servicio del que XCS de WatchGuard es propietario y donde podemos ver el status de una IP o de un servidor de correo a través de su domino.

Integración con F5

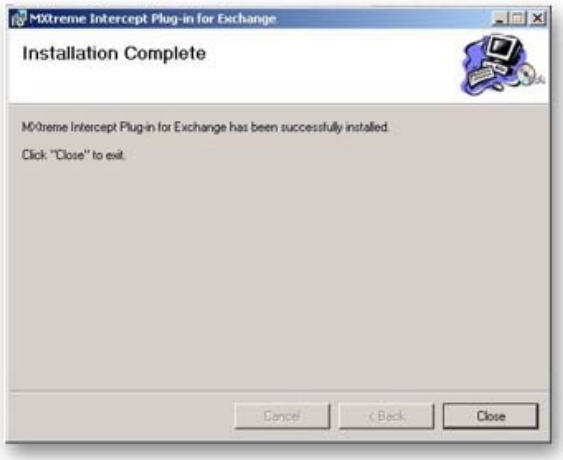
Si se dispone de balanceadores de carga de F5, se puede integrar XCS de WatchGuard con su infraestructura de forma que:

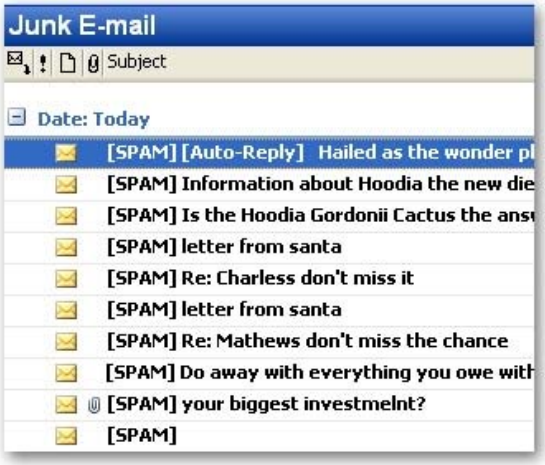


- Reduce el tráfico de correo-e bloqueándolo antes de que alcance el cortafuegos de correo-e vía las políticas creadas por XCS Email Firewall
- Conexiones entrantes bloqueadas en el mismo perímetro de la red
- Envía datos de prevención de amenazas a los equipos de infraestructura de red
- Incrementa la Calidad del Servicio reduciendo el correo-e en más del 70%

Plugins para Exchage

Si disponen de servidores de correo Exchange, XCS Email Firewall de XCS de WatchGuard dispone de un adaptador que facilita la administración del entorno.



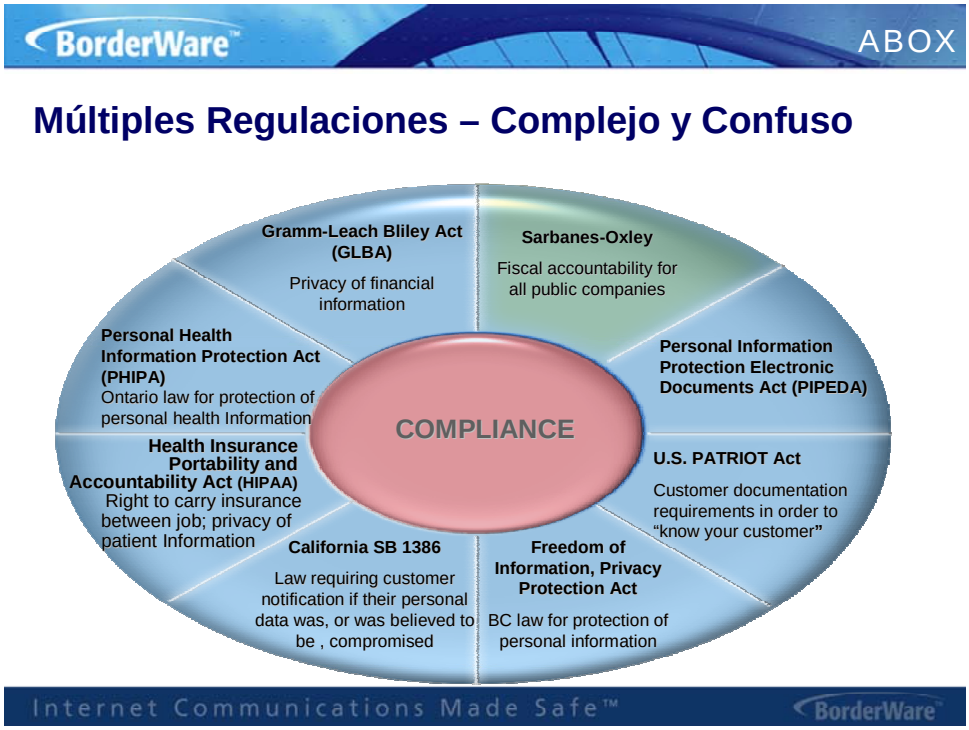


Control de Ataques

Se trata de minimizar la posibilidad de fuga de información confidencial de la empresa, esto es muy importante para empresas con nivel de seguridad alta como son los entornos Hospitalarios, Empresas de Seguros, Banca, etc. XCS Email Firewall nos permite realizar:

- Control de contenido Saliente.
- Cumplir con Regulaciones.
- Protección Info Confidencial.
- Mitigar Riesgos Legales.

Se trata de Reforzar Políticas Corporativas y Reducir Responsabilidades Legales. El entorno legal es realmente complicado con legislaciones en distintos países y XCS de WatchGuard con XCS Email Firewall ha conseguido dar una solución útil para todos estos países y entornos legales.



Retos Empresa

- Evitar exponerse a riesgos
- Evitar sanciones civiles o criminales
- Preparar evidencias para investigaciones y procesos judiciales
- Evitar mala publicidad y gastos asociados y pérdida de negocio
- Proteger clientes
- Promover responsabilidad legal

Retos técnicos que XCS Email Firewall ha solucionado

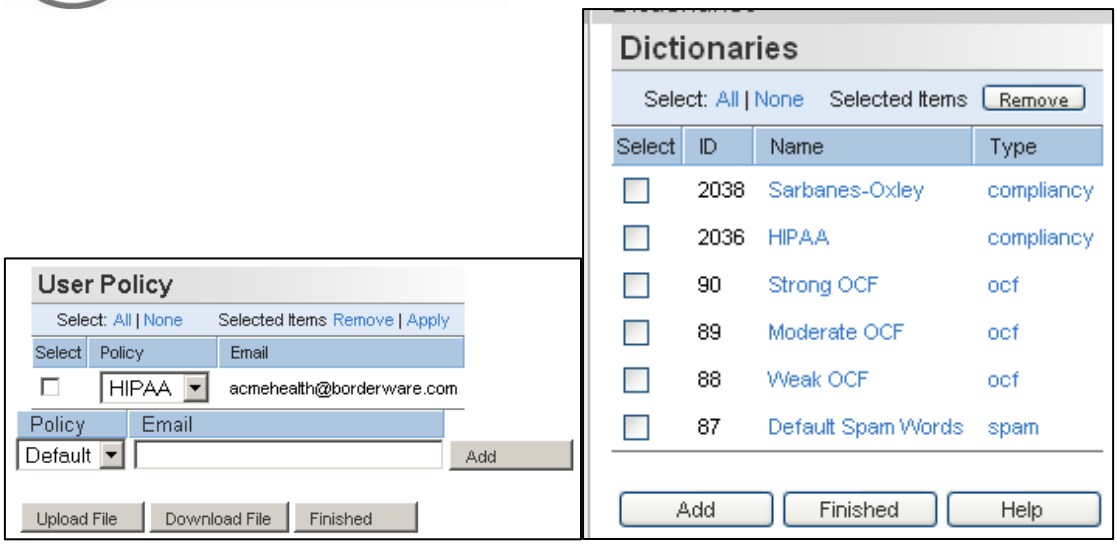
- Servicio de mensajería fiable y altamente disponible
- Controles de Encriptación y autenticación
- Protección contra virus, spam y tráfico no autorizado
- Controles basados en Políticas para bloquear, redirigir y archivar mensajes de acuerdo con las directrices internas y las normas regulatorias, p.e.: UNE-17999

WatchGuard

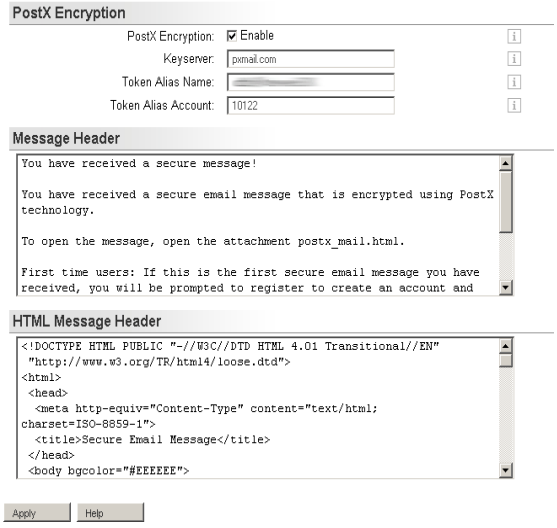
Motor de Privacidad y conformidad de XCS Email Firewall

Gestor de contenidos

- Reglas de filtrado avanzado de correo-e
  - Políticas basadas en usuario, grupo y dominio
  - Granularidad completa sobre funciones de correo-e
- Inspección de contenido incluye
  - Habilidad para escanear el contenido del mensaje de correo-e, incluyendo los adjuntos
- Diccionarios
  - Soporte de múltiples diccionarios (OCF) con diccionarios pre-definidos para pornografía, groserías y spam
  - Específicos para cumplir con HIPAA, GLBA, SOX
  - Configurables/personalizables por usuario



Privacidad & Conformidad – Integración PostX



- Proporciona una solución única para privacidad y conformidad
- Encriptación PostX integrada directamente en XCS Email Firewall
  - No necesita un segundo sistema
- Sistema único de política, gestión, informes y registro
- Elimina la tediosa tarea de administrar las claves de encriptación
- El mensage se envía como un adjunto encriptado para ser bajado.
- El mensaje se visualiza después de que el usuario proporciona sus credenciales

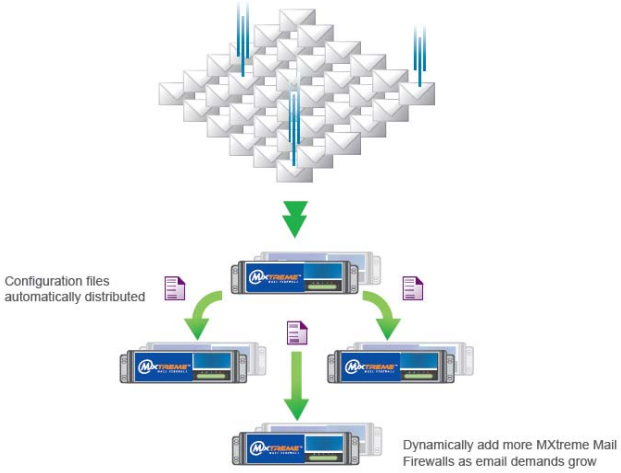
Gestión de XCS Email Firewall

El disponer de Alta Disponibilidad es muy sencillo de poner en marcha, los elementos distribuyen la carga de trabajo de forma dinámica, ofreciendo una solución con las siguientes características:

- Redundancia a nivel de mensaje & tolerancia a fallos con replicación de cola. **Es una patente de XCS de WatchGuard**

- Replica la cola de correo-e en el equipo cluster para asegurar que los mensajes no se pierden

- Clustering On-Demand
  - Única solución para grandes compañías y proveedores de servicio que soportan entornos de correo-e críticos.
  - La configuración de un appliance se distribuye de forma automática a los elementos que se agregan.
  - Escalabilidad y redundancia a nivel de mensaje.



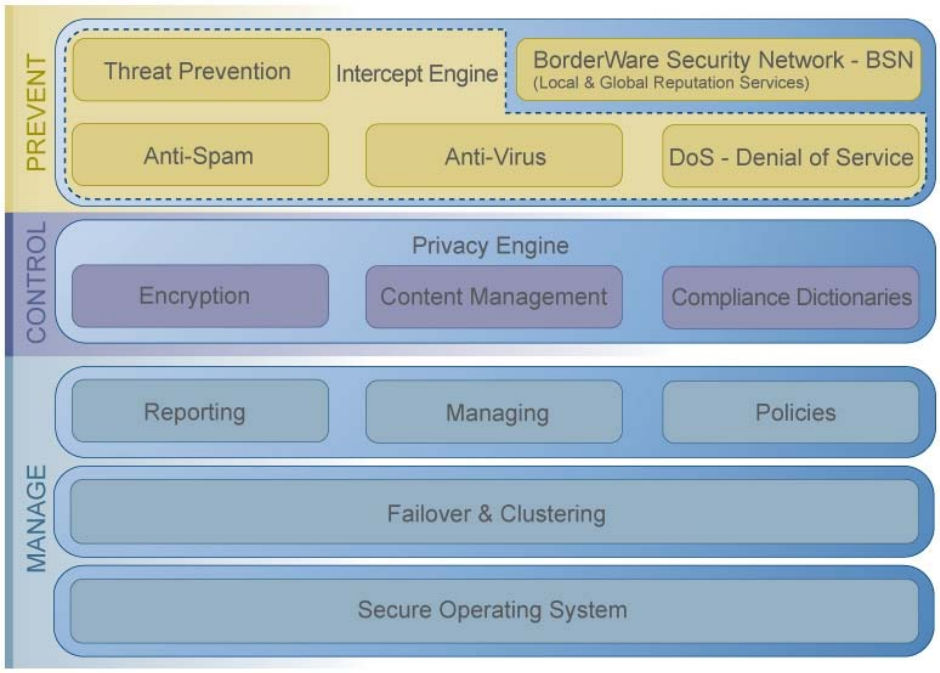
- WebMail Seguro
  - Acceso remoto seguro al correo-e
- Integración LDAP
  - Administración y gestión centralizada
- Informes
  - Motor de informes, logs y histórico de correo-e configurable

Generación de Informe

Todas las solución de seguridad deben de permitir monitorizar que esta sucediendo en cualquier momento, XCS Email Firewall dispone de un potente modulo de monitorización y de informes que permiten el control de lo que ocurre en todo momento, con un sistema de alarmas configurables.

View, Generate and Configure Reports
Report Name
Configure
Generate
Full Report
Configure
Generate
HIPAA Compliance Report
Configure
Generate
Add New Report Type
Delete Selected Report Type
Help

La arquitectura de XCS Email Firewall



Necesidades y solución Técnica

Podemos cumplir con todas las especificaciones, no se puede garantizar el 0% de falsos negativos, (nadie lo puede garantizar), el sistema es totalmente escalable y no hay problema para las 20.000 cuentas de correo (no hay limite en el numero de cuentas) y tratar hasta 15.000.000 de correos al mes lo podemos hacer un MX-400.

La oferta económica

El modelo MX-400 de XCS de WatchGuard ofrece un rendimiento que permite tratar hasta 32.500 mail por hora. El cluster nos va a permitir por lo tanto el tratamiento de 65.000 mail por hora, si multiplicamos por 24 horas de un día y los 30 días del mes, son esta solución se pueden tratar hasta 65.000 mails / hora x 24 horas / día x 30 días x 1 mes = 46.800.000 millones de emails por mes. En el caso de fallo de uno de los equipos del cluster, se pueden seguir procesando sin problemas 23.400.000 email al mes.