Ministerio de Agricultura y Desarrollo Rural

CONTROLES DE SEGURIDAD PARA LOS SERVICIOS TECNOLÓGICOS

V 1.0

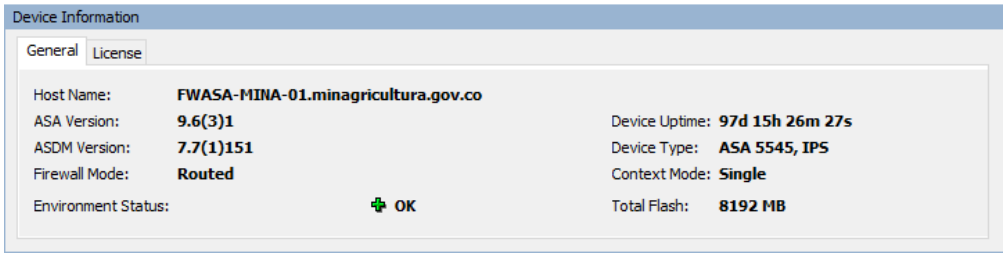
Especialista en Redes y Seguridad
08/11/2017
Bogotá, Colombia

DISPOSITIVOS DE SEGURIDAD MINISTERIO DE AGRICULTURA

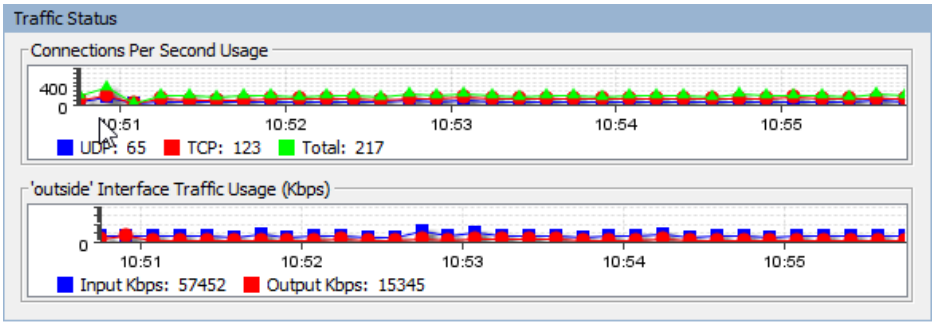
El Ministerio de Agricultura y Desarrollo Rural (en adelante MinAgricultura), cuenta actualmente a nivel de seguridad con los siguientes dispositivos y Software:

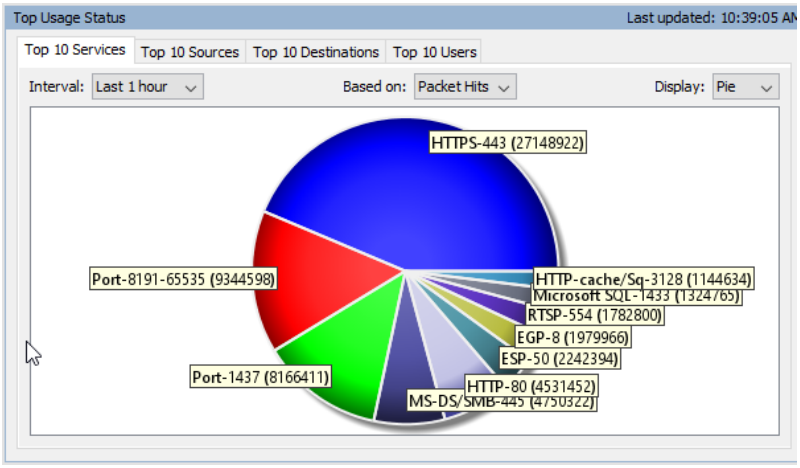
1. Firewall Perimetral (dos dispositivos en alta disponibilidad)

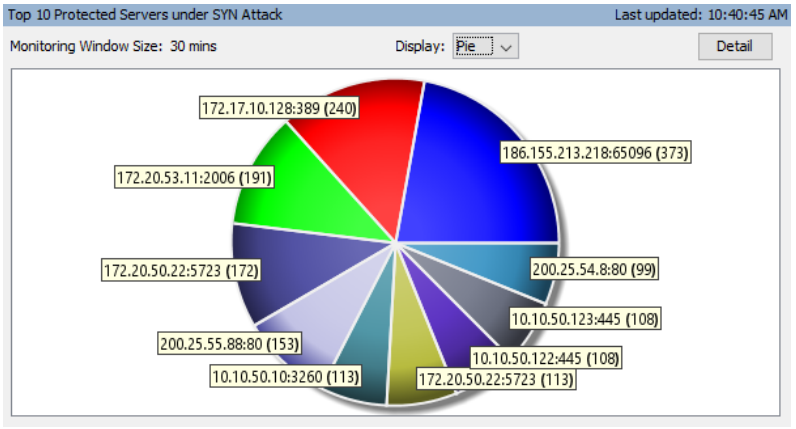
Actualmente se cuenta con dos firewalls Cisco 5545 en alta disponibilidad para protección del perímetro de la red de MinAgricultura.




```
Stateful Failover Logical Update Statistics
        Link : FAILOVER GigabitEthernet0/7 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         2503131518 0          1124012    0
        sys cmd         1124014    0          1124012    0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1699503447 0          0          0
        UDP conn        702757997  0          0          0
        ARP tbl         97346458   0          0          0
        Xlate Timeout   0          0          0          0
```

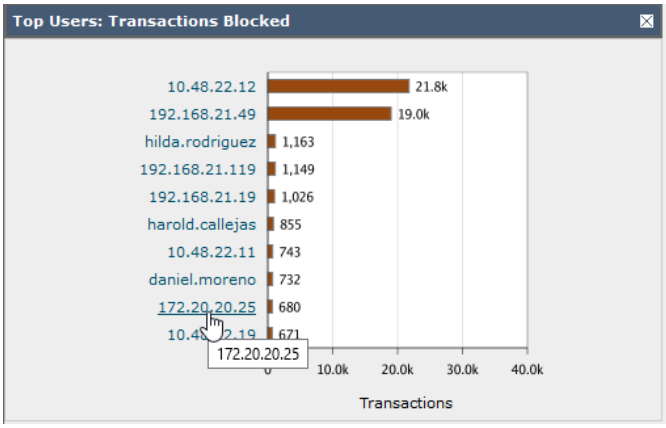


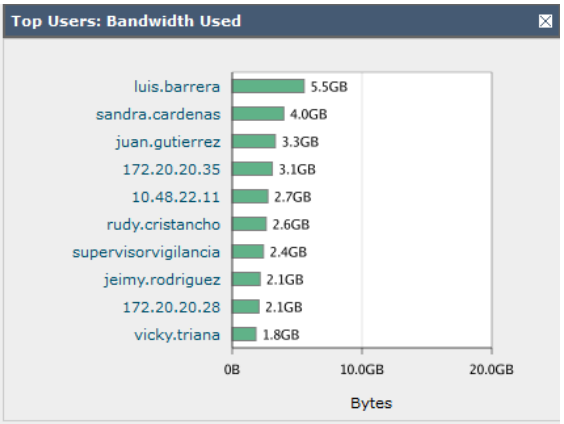




2. WSA Web Security Appliance (dos dispositivos)

Actualmente se cuenta WSA los cuales permiten una detección avanzada de amenazas, visibilidad de aplicaciones y control y filtrado de contenido web.



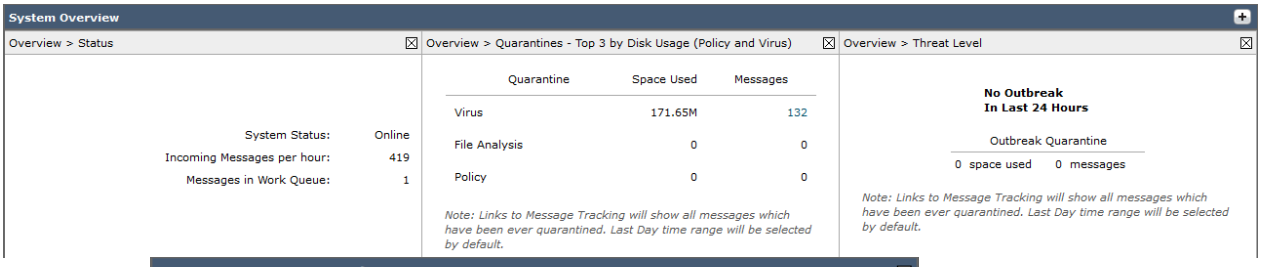


Overview > Web Proxy Summary

	%	Transactions
Suspect Transactions	9.0%	76.0k
Clean Transactions	91.0%	768.3k
Total Transactions:		**844.3k**

3. ESA Email Security Appliance (dos dispositivos en alta disponibilidad)

Minagricultura cuenta con un gateway de seguridad para correo electrónico, este dispositivo detecta y bloquea una amplia variedad de amenazas al correo electrónico, tales como malware, spam e intentos de phishing.

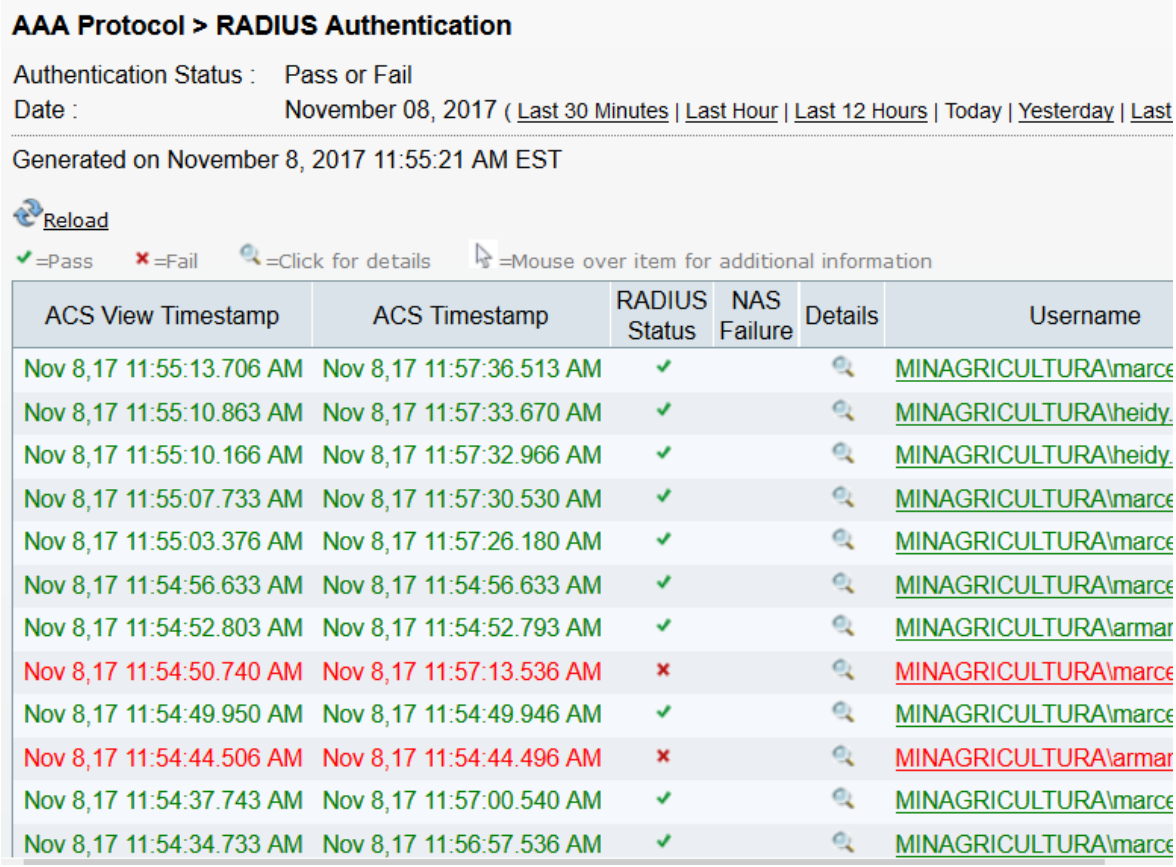


Overview > Incoming Mail Summary

Message Category	%	Messages
Stopped by Reputation Filtering	69.1%	3,812
Stopped as Invalid Recipients	6.7%	369
Spam Detected	4.6%	255
Virus Detected	0.1%	4
Detected by Advanced Malware Protection	0.0%	0
Messages with Ma icious URLs	0.0%	0
Stopped by Content Filter	0.0%	0
Stopped by DMARC	0.0%	0
S/MIME Verification/Decryption Failed	0.0%	0
Total Threat Messages:	**80.5%**	**4,440**
Marketing Messages	3.2%	179
Social Networking Messages	0.6%	35
Bulk Messages	2.9%	160
Total Graymails:	**6.8%**	**374**
S/MIME Verification/Decryption Successful	0.0%	0
Clean Messages	12.7%	700
Total Attempted Messages:		**5,514**

4. ACS Access Control System (dos dispositivos en alta disponibilidad)

El Ministerio cuenta con Un Sistema de administración de identidad y centralizando en el control de admisión basado en la red. Tras confirmar la identidad de un usuario o dispositivo, así como su cumplimiento de la política de seguridad de la entidad. La red es responsable de la identificación, autorización y cumplimiento por medio de protocolos de autenticación como 802.1X y funciones AAA (autenticación, autorización y contabilidad) además de la posibilidad de bloquear completamente todo acceso no autorizado.



AAA Protocol > RADIUS Authentication

Authentication Status : Pass or Fail
Date : November 08, 2017 (Last 30 Minutes | Last Hour | Last 12 Hours | Today | Yesterday | Last

Generated on November 8, 2017 11:55:21 AM EST

Reload

✔=Pass ✖=Fail =Click for details =Mouse over item for additional information

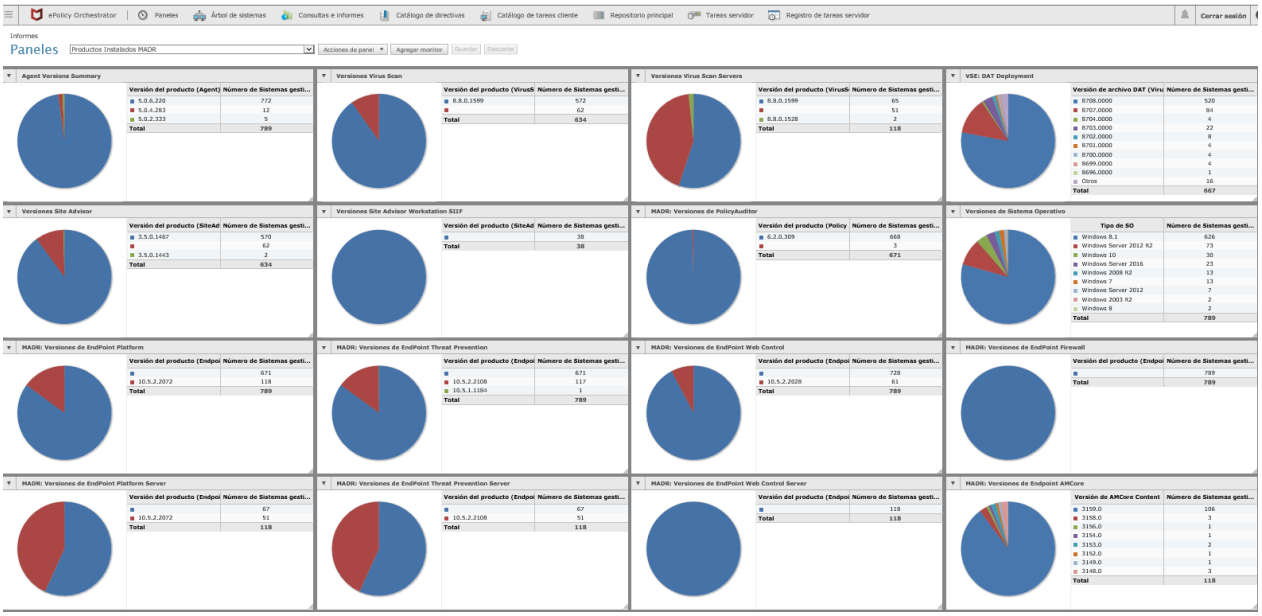
ACS View Timestamp	ACS Timestamp	RADIUS Status	NAS Failure	Details	Username
Nov 8,17 11:55:13.706 AM	Nov 8,17 11:57:36.513 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:55:10.863 AM	Nov 8,17 11:57:33.670 AM	✔			MINAGRICULTURA\heidy.
Nov 8,17 11:55:10.166 AM	Nov 8,17 11:57:32.966 AM	✔			MINAGRICULTURA\heidy.
Nov 8,17 11:55:07.733 AM	Nov 8,17 11:57:30.530 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:55:03.376 AM	Nov 8,17 11:57:26.180 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:54:56.633 AM	Nov 8,17 11:54:56.633 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:54:52.803 AM	Nov 8,17 11:54:52.793 AM	✔			MINAGRICULTURA\armar
Nov 8,17 11:54:50.740 AM	Nov 8,17 11:57:13.536 AM	✖			MINAGRICULTURA\marce
Nov 8,17 11:54:49.950 AM	Nov 8,17 11:54:49.946 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:54:44.506 AM	Nov 8,17 11:54:44.496 AM	✖			MINAGRICULTURA\armar
Nov 8,17 11:54:37.743 AM	Nov 8,17 11:57:00.540 AM	✔			MINAGRICULTURA\marce
Nov 8,17 11:54:34.733 AM	Nov 8,17 11:56:57.536 AM	✔			MINAGRICULTURA\marce

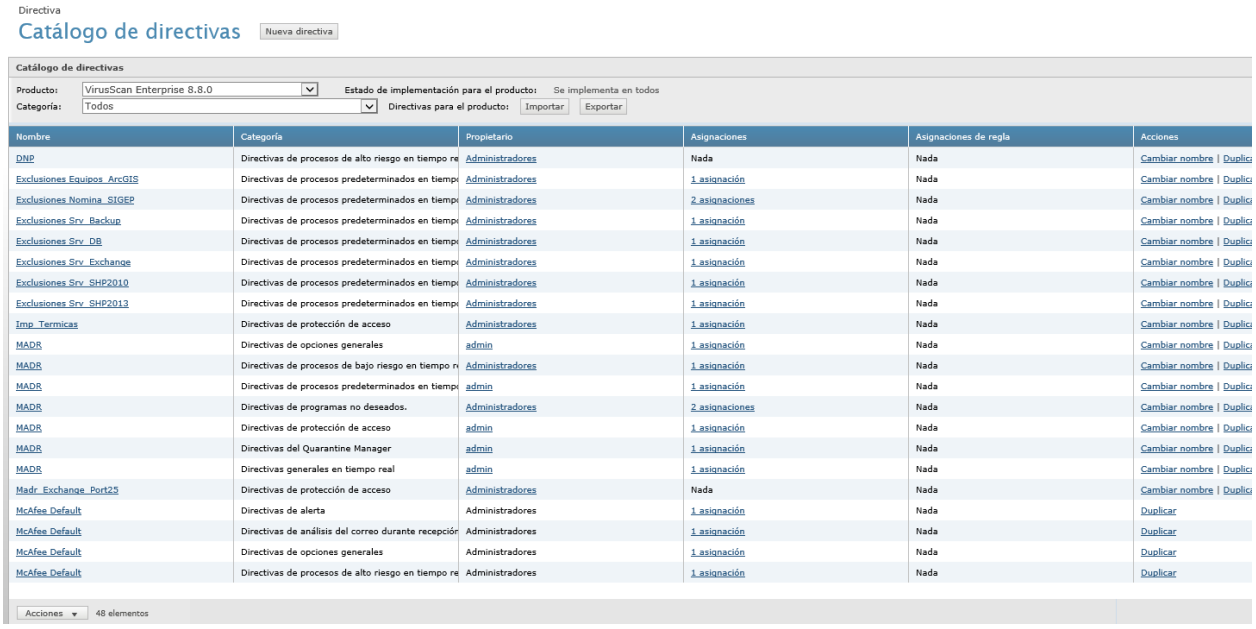
5. Seguridad del Antivirus

McAfee ePolicy Orchestrator es una plataforma amigable que permite de forma controlada la administración e implementación centralizada de directivas en los productos de seguridad y los sistemas en los que se encuentren instalados.

Ofrece distintas funciones de generación de informes y despliegue de productos desde un único punto de control. Además, permite administrar los productos de seguridad para equipos y servidores a través de la implementación de directivas de seguridad y la creación de tareas automáticas.

Los archivos de definición de detecciones (DAT), motores antivirus y otros contenidos de seguridad se actualizan diariamente para garantizar la protección de los sistemas gestionados.





Directiva

Catálogo de directivas [Nueva directiva]

Catálogo de directivas

Producto: VirusScan Enterprise 8.8.0 — Estado de implementación para el producto: Se implementa en todos

Categoría: Todos — Directivas para el producto: [Importar] [Exportar]

Nombre	Categoría	Propietario	Asignaciones	Asignaciones de regla	Acciones
DNP	Directivas de procesos de alto riesgo en tiempo re	Administradores	Nada	Nada	Cambiar nombre | Duplic
Exclusiones Equipos ArcGIS	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Exclusiones Nomina SIGEP	Directivas de procesos predeterminados en tiemp	Administradores	2 asignaciones	Nada	Cambiar nombre | Duplic
Exclusiones Srv Backup	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Exclusiones Srv DB	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Exclusiones Srv Exchange	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Exclusiones Srv SHP2010	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Exclusiones Srv SHP2013	Directivas de procesos predeterminados en tiemp	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
Imp Termicas	Directivas de protección de acceso	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas de opciones generales	admin	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas de procesos de bajo riesgo en tiempo r	Administradores	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas de procesos predeterminados en tiemp	admin	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas de programas no deseados.	Administradores	2 asignaciones	Nada	Cambiar nombre | Duplic
MADR	Directivas de protección de acceso	admin	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas del Quarantine Manager	admin	1 asignación	Nada	Cambiar nombre | Duplic
MADR	Directivas generales en tiempo real	admin	1 asignación	Nada	Cambiar nombre | Duplic
Madr Exchange Port25	Directivas de protección de acceso	Administradores	Nada	Nada	Cambiar nombre | Duplic
McAfee Default	Directivas de alerta	Administradores	1 asignación	Nada	Duplicar
McAfee Default	Directivas de análisis del correo durante recepción	Administradores	1 asignación	Nada	Duplicar
McAfee Default	Directivas de opciones generales	Administradores	1 asignación	Nada	Duplicar
McAfee Default	Directivas de procesos de alto riesgo en tiempo re	Administradores	1 asignación	Nada	Duplicar

Acciones — 48 elementos