
SOPHOS
FIREWALL
GUÍA DE COMANDOS
Digital User
Ciberseguridad para todos

SOPHOS XG - COMANDOS ÚTILES (DEVICE CONSOLE) OP.4

MUESTRA LOS PAQUETES "DROPIADOS" POR EL FIREWALL
drop-packet-capture -> host | src host | dst host | net | src net | dst net | port | proto | or, and, not

CAPTURA Y ANÁLISIS DE TRÁFICO
tcpdump ' ' -> host | net | src net | dst net | port | port not | src port | dst port | proto | interface | and, or..

MUESTRA LA PRIORIDAD DE ENRRUTAMIENTO
system route_precedence show

CONFIGURA LA PRIORIDAD DE ENRRUTAMIENTO
system route_precedence set static sdwan_policyroute vpn

MUESTRA INFORMACIÓN DEL FW (SERIAL, MODELO, FIRMWARE...)
system diagnostics show version-info

CONSUMO DE ANCHO DE BANDA EN TIEMPO REAL X INTERFAZ
system diagnostics utilities bandwidth-monitor

CANTIDAD DE CPU Y RAM UTILIZADA X PROCESO (MONITOR DE PROCESOS)
system diagnostics utilities process-monitor

REALIZA UN BYPASS A LA CONFIGURACIÓN DE ACCESO AL DISPOSITIVO
system appliance_access enable

PING DESDE UNA INTERFAZ EN ESPECIFICO
ping sourceip 201.236.25.42 190.25.23.1

¿A QUÉ PAÍS PERTENECE UNA DIRECCIÓN IP?
show country-host ip2country ipaddress 52.67.251.104

MUESTRA ALGUNOS PARAMETROS DE RED CONFIGURADOS
show network -> interfaces | static-route | mtu-mss | macaddr | lag-interface | interface-speed

HACER QUE EL TRÁFICO DE SALIDA Y RETORNO NO PASE POR EL FW PARA UN DETERMINADO HOST O RED
set advanced-firewall bypass-stateful-firewall-config add source_host 172.16.16.20 dest_host 201.236.24.32

REINICIAR EL FW
system shutdown

Síguenos en Facebook
ACADEMIA SOPHOS EN ESPAÑOL

Digital User
Ciberseguridad para todos

SOPHOS XG
VPN SITE-TO-SITE
ERRORES Y POSIBLES CAUSAS

LOG DEL SERVICIO IPSEC VPN
tail -f /log/strongswan.log

¿CÓMO ESTÁN LAS SA (SECURITY ASSOCIATION)?
ipsec statusall

VER LAS POLÍTICAS DE TRANSFORMACIÓN
ip xfrm policy

RECEIVED NO_PROPOSAL_CHOSEN ERROR NOTIFY
- El peer remoto está rechazando "la propuesta" en la fase 1 o la fase 2.
- Las políticas de cifrado, autenticación y grupo de DH deben hacer match.
- La dirección IP (Peer) debe hacer match también.

RECEIVED AUTHENTICATION_FAILED
- Fallamos en autenticarnos ante el Peer remoto.
- El Peer remoto esperaba un "Peer ID" diferente. Ej. Nombre de DNS en lugar de la IP (x defecto).
- Valida si hay dispositivos intermedios que puedan alterar la IP "que ve cada extremo".
- Configura el "Peer ID" en ambos FW de forma que hagan match.

IGNORE MALFORMED INFORMATIONAL REQUEST
- El campo información de la petición IKE está malformado o no se puede leer.
- Verifica que la preshared key es igual en ambos Peers.
- Verifica con el ISP si su dispositivo puede estar dañando los paquetes.
- Prueba de ser posible la conexión con otro ISP.
- Válida que la MTU y MSS hacen match con el del ISP (WAN).

RECEIVED INVALID_ID_INFORMATION ERROR NOTIFY
- Verifica las redes configuradas en cada Peer.

LA VPN "SUBE" DE FORMA INESTABLE
- La configuración del "lifetime" no hace match en ambos Peers.
- Sophos FW no soporta "re-keying" basado en tráfico, así que valida que el Peer remoto no lo tenga habilitado.

Síguenos en Facebook
ACADEMIA SOPHOS EN ESPAÑOL

Digital User
Ciberseguridad para todos

Digital User

Ciberseguridad para todos

SOPHOS XG ADVANCED SHELL COMANDO DE HOY

bwmon

- Muestra el ancho de banda de cada interfaz en el XG.
- Los resultados x defecto están en KBytes/s.

En el teclado

+ Incrementa el tiempo de muestreo en 100ms.

- Disminuye el tiempo de muestreo en 100ms.

U Ciclo: bytes, bits, paquetes, errores.

T Ciclo: tasa actual, máx, suma desde el inicio, promedio de los últimos 30 seg.

Síguenos en Facebook

ACADEMIA SOPHOS EN ESPAÑOL

```
Bandwidth Monitor, (Sampling at every 0.500s), press 'h' for help

-         iface                   Rx                   Tx                Total
==============================================================================
          Port1:          0.00 KB/s            0.00 KB/s            0.00 KB/s
        GuestAP:          0.00 KB/s            0.00 KB/s            0.00 KB/s
            lo:         15.49 KB/s           15.49 KB/s           30.97 KB/s
         ipsec0:          0.00 KB/s            0.00 KB/s            0.00 KB/s
          tun0:          0.00 KB/s            0.00 KB/s            0.00 KB/s
          Port2:          0.22 KB/s            0.33 KB/s            0.54 KB/s
           imq0:          0.00 KB/s            0.00 KB/s            0.00 KB/s
------------------------------------------------------------------------------
         total:         15.71 KB/s           15.81 KB/s           31.52 KB/s
```

Digital User

Ciberseguridad para todos

SOPHOS XG ADVANCED SHELL COMANDO DE HOY

drppkt

- Muestra los paquetes "quemados" por el firewall.
- Muestra los detalles de la conexión y paquetes procesados.

Filtros

host | src host | dst host | net | src net | dst net | port | src port | dst port
port not | proto ICMP | proto UDP | proto TCP | arp

Ejemplos

drppkt src host 192.168.1.10
drppkt net 192.168.1
drppkt port 3389
drppkt host 192.168.1.90 and port not 21
drppkt proto ICMP
drppkt arp

Síguenos en Facebook
ACADEMIA SOPHOS EN ESPAÑOL

```
SFVH_SO01_SFOS 18.5.1 MR-1-Build326# drppkt 172.16.16.20
drppkt: Invalid filter "172.16.16.20"
SFVH_SO01_SFOS 18.5.1 MR-1-Build326# drppkt host 172.16.16.20
2022-04-19 19:32:50 0101021 IP 172.16.16.20.49201 > 186.233.185.146.6568 : proto TCP: S 1016342293:1016342293(0) win 8192 checksum : 57580
0x0000:  4500 0034 0a5b 4000 7f06 c0c8 ac10 1014  E..4.[@.........
0x0010:  bae9 b992 c031 19a8 3c94 2715 0000 0000  .....1..<.'.....
0x0020:  8002 2000 e0ec 0000 0204 05b4 0103 0308  ................
0x0030:  0101 0402                                ....
Date=2022-04-19 Time=19:32:50 log_id=0101021 log_type=Firewall log_component=Firewall_Rule log_subtype=Denied log_status=N/A log_priority=A
e_id=1 outzone_id=2 source_mac=08:00:27:7e:ca:10 dest_mac=00:1a:8c:37:86:18 bridge_name= l3_protocol=IPv4 source_ip=172.16.16.20 dest_ip=186
st_port=6568 fw_rule_id=0 policytype=0 live_userid=0 userid=0 user_gp=0 ips_id=0 sslvpn_id=0 web_filter_id=0 hotspot_id=0 hotspotuser_id=0
_id=0 app_category_id=0 app_id=0 category_id=0 bandwidth_id=0 up_classid=0 dn_classid=0 nat_id=0 cluster_node=0 inmark=0x0 nfqueue=0 gatewa
 state=1, flag0=36029346776875008 flags1=0 pbdid_dir0=0 pbrid_dir1=0
```

Digital User

Ciberseguridad para todos

SOPHOS XG ADVANCED SHELL COMANDO DE HOY

Síguenos en Facebook

ACADEMIA SOPHOS EN ESPAÑOL

conntrack

- Lista las conexiones en Sophos Firewall.
- Nos ayuda a identificar los ID de cada paquete en el tráfico procesado.

Ejemplo

- conntrack -L -s 192.168.1.10 -d 8.8.8.8
- Mostrará el tráfico generado desde la 1.10 hacia la 8.8.8.8.

Algunos Párametros

-s	dirección ip de origen
-d	dirección ip de destino
-p	Protocolo ej. tcp
-f	familia del protocolo ej. ipv6

Algunos Campos

fwid	id de la regla de firewall
idp	id de la política de IPS
webfiltid	id de la política de filtrado web
appfiltid	id de la política de filtrado de aplicaciones
snatid	id de la política de source nat
svp	id de la política de SSLVPN
bwid	id de la política de ancho de banda

NOTA

Si el fwid es Cero ej. fwid-0 significa que el tráfico es generado por el mismo firewall (en la mayoria de casos).

SOPHOS XG
SE ME VENCIÓ LA LICENCIA
¿QUÉ QUEDA ACTIVADO?

¿QUEDO CON INTERNET?

SI -> DNS | DNS Dinámico | DHCP | VLAN DHCP | VLAN Bridge | NTP | IPv6 Tunneling | Jumbo Frame | Routing (Estático, Multicast y Dinámico) | NAT | Stateful Firewall | SNMP | CLI | Firmware Update

¿QUEDO CON DESCIFRADO?

SI -> Inspección SSL / TLS, sin embargo el escaneo y bloqueo de Malware se encuentra dentro de la subscripción de WEB PROTECTION.

¿QUEDO CON BALANCEO DE ENLACES WAN?

SI -> Failover Automático | Multipath Rules | Ruteo de aplicaciones por enlaces específicos | Túnel RED de capa 2 con routing | Synchronized SD-WAN | Centralized VPN Orchestration | Soporte para múltiples enlaces WAN (VDSL, DSL, Cable, 3G/4G/LTE Cellular)

¿QUÉ PASA CON MIS VPN?

Todas activadas (S2S, SSL, L2TP, PPTP, Sophos Connect, Sophos RED S2S) menos las "Clientless VPN" que funciona con el portal de autoservicio HTML5 y hace parte de la subscripción de Network Protection.

¿QUÉ SUCEDE CON MIS SERVICIOS DE AUTENTICACIÓN?

Todos quedan activos - Synchronized user ID | Active Directory, eDirectory, RADIUS, LDAP, TACAC's | STAS | SATC | Agentes de autenticación | Google Chromebook Auth | Servicios de autenticación para Ipsec, SSL, l2TP, PPTP | Doble factor de autenticación (OTP).

Y LOS AP'S - WIRELESS

Todo queda activado -> Gestión de los AP's | Fast Transition | Hotspot | Mesh Networks...

¿PUEDO APLICAR REGLAS DE QOS?

Si pero solo por red o usuario - No podrás aplicarlo por aplicaciones o categorías WEB esta funcionalidad hace parte de la subscripción de WEB PROTECTION.

¿QUÉ SUCEDE CON MI HA?

Funcionará sin problemas para 2 dispositivos en activo-activo o activo-pasivo.

ADMINISTRACIÓN EN SOPHOS CENTRAL

Reporte para múltiples FW | últimos 5 archivos de backup | Actualizaciones de firmware | Backup de Logs | Sophos MTR Connector | Despliegue Zero-Touch

Síguenos en Facebook
ACADEMIA SOPHOS EN ESPAÑOL

Digital User
Ciberseguridad para todos