Security Automation

Connecting Your Silos

Lisa Lorenzin
Principal Solutions Architect
Juniper Network
A Babel Fish diagram illustrating its various internal components. The text beneath the diagram reads:

THE BABEL FISH IS SMALL, YELLOW, LEECHLIKE, AND PROBABLY THE ODDEST THING IN THE UNIVERSE.
XML > SOAP > HTTPS
Compliance Check

Non-compliant System
Windows 7
• Self-Encrypting Drive
• AV - McAfee VirusScan 8.0
• Firewall

Compliant System
Windows 7
• Self-Encrypting Drive
• AV - Symantec Endpoint Protection 11.0
• Firewall

Security Policy
Windows 7
• Self Encrypting Drive
• AV (one of)
  • Symantec Endpoint Protection 11.x
  • McAfee VirusScan 8.x
• Firewall
Endpoint

Enforcement Point

Policy Server

MAP

MAP Clients

- Remediation Network

Security Policy
- No P2P file sharing
- No spamming
- No attacking others
NAC Is Not Dead
Often Infected

Robert Smith

Funniest video ever! Check out the link!

Click Here

MALWARE SITE

Email

Intranet

Corporate Financial Data

Can’t inspect content in network

Can’t control access to sensitive data

Can’t protect user from cloud-based threats

Doesn’t have Intelligence to detect Malware on Client

Connected To Corporate Network

Can’t protect user from cloud-based threats

Email

Intranet

Corporate Financial Data

Can’t inspect content in network

Can’t control access to sensitive data

Doesn’t have Intelligence to detect Malware on Client
Robert Smith

Funniest video ever! Check out the link!

Click Here

MALWARE SITE
Email
Intranet
Corporate Financial Data

CAN detect malware on the client

CAN enforce access via user, location and device context

CAN coordinate security to provide access control to sensitive information

CAN enable Client traffic directed to Cloud, CAN scrub and detect malware

9/29/2014
Copyright 2014 Trusted Computing Group
identity = john.smith

role=finance and employee

authenticated-as

access-request-mac

mac-address=00:11:22:33:44:55

ip-mac

ip-address = 10.99.99.32

ip-address = 192.168.0.7

ip-mac

layer2-information
VLAN=978
Port=12

access-request = 111:33

layer2-information
VLAN=978
Port=12

authenticated-by

device-attribute = av-signatures-out-of-date

location = HQ

device = 111:3

device-ip

ip-address = 10.0.0.5

device-ip

device = 111:0

device-ip

ip-address = 10.0.0.6

device-ip

device = 111:55

access-request-device
IF-MAP Event Messages

Endpoint

Enforcement Point

Policy Server

MAP

MAP Clients

9/29/2014 Copyright 2014 Trusted Computing Group
• TNC & IF-MAP
  – IF-MAP Standards & FAQ
    • http://www.trustedcomputinggroup.org/community/2014/03/ifmap_22__learning_from_experience
    • http://www.trustedcomputinggroup.org/resources/tnc_ifmap_binding_for_soap_specification
    • http://bit.ly/KKpdDx
  – Mobile Security Architects Guide
    • http://www.trustedcomputinggroup.org/resources/architects_guide_mobile_security_using_tnc_technology
  – Security Automation Architects Guide
    • http://www.trustedcomputinggroup.org/resources/tcg_security_automation_architects_guide
Lisa Lorenzin
llorenzin@juniper.net