SECURING NEW CAMPUS AND BRANCH NETWORK, PREPARING FOR BYOD AND BYOA

Phal Nanda
PREPARING FOR BYOD
MAJOR MARKET TRENDS...
DATA MOBILITY AND SCALE AT AN ALL TIME HIGH AND GROWING

Device Proliferation

New Devices

Explosion of Devices

14B

5B

*Forester

Diversity of Applications and Richness Of Data

New Applications

Security Risk Proliferation

Type of Attack

Sophistication (Maturity)

Virus

Worms

Trojans

DoS

Malware

Botnets

APT
CAMPUS MOBILITY TRENDS

Unique Daily Wireless Sessions
Large American University ~50,000 Students, Multiple Devices Per Student

Top WLAN requirements
BYOD
Unified Policy
Performance at Scale
Highly Resilient
High Density
High Scale
MOBILITY IS MUCH MORE THAN BYOD

Today's business environment requires coordinated access

Guest Devices

Employee Owned Devices (BYOD)

Corporate Owned Devices
Guests gain access, IT gains granular control over network usage.

Access denied!

This hospital is reserving bandwidth for what matters most.
1. Unknown device connects to open captive portal SSID

2. User session is captured and redirected to SmartPass

3. User selects SmartPass self-registration and creates a temporary user credential

4. SmartPass sends temporary credential to end user via Clickatell SMS service

5. User uses temporary credentials to authenticate against SmartPass

6. User is connected to the network using mobile phone number and temporary password
GUEST USER ON CORPORATE NETWORK
APPLICATION RESTRICTION

1. Device authenticates on wireless network
   - Wireless User Tablet/smartphone

2. Smartpass communicates user and IP information to UAC via IF-MAP
   - AP
   - EX Series

3. UAC pushes role based ACL and FW policies to EX, WL and SRX
   - UAC

4. SRX enforces user policies allowing user basic access to all servers except finance
   - SRX
   - SmartPass

5. SRX AppSecure Polices block bandwidth intensive applications like YouTube Video
   - Corporate Data Center
   - Apps
   - Data
   - Finance
   - Video
   - Internet

   - Active Directory /LDAP
   - EX Series
   - SmartPass
   - UAC
   - WLC
   - SRX
Employees use their own device to simply access secure network, IT can limit use to business critical functions.

Access denied!
This hospital is reserving bandwidth for what matters most!

Hospital Network
- WLA532
- WLC2800
- W/SMARTpass
- Provisioning Server
- SRX 550
- Junos Pulse Access Control Service (UAC)

Guest Devices
- Employee Owned
- Corporate Owned
EMPLOYEE OWNED DEVICE ON CORPORATE NETWORK
EMPLOYEE SELF PROVISIONING

1. Unknown device connects to open captive portal SSID

2. User session is captured and redirected to SmartPass

3. SmartPass web portal presents captive portal and redirects client to provisioning server

4. Provisioning server pushes native supplicant config wizard to client device

5. Provisioning server gets user credentials from wizard; validates against AD; and requests user cert for end user

6. Provisioning wizard gets EAP-TLS configuration profile (and cert) from provisioning server; agent dissolves

7. User selects secure wireless network and device authenticates to RADIUS without requiring user to enter credentials
EMPLOYEE OWNED DEVICE ON CORPORATE NETWORK
APPLICATION RESTRICTION

1. Device authenticated on wireless network

2. DHCP Server/SmartPass communicates User and IP information to UAC via IF-MAP

3. UAC pushes role based ACL and FW policies to EX and SRX

4. SRX enforces user policies allowing user basic access to all servers except finance

5. SRX AppSecure Polices block non-work related applications like Hulu and Netflix

SRX AppTrack feature combined with MAG data collects per user application information providing detailed reports in STRM
SMARTPASS IFMAP SUPPORT

SmartPass 7.7 adds support for two IF-MAP use cases

- **Guest User Federation** – Guest users authenticating with SmartPass have complete session information published to IF-MAP; UAC can apply dynamic policy based on “learned” sessions

- **IP-MAC Binding for Non-agented Dot1x Sessions** – Dot1x users authenticate directly with UAC; WLC sends session IP-MAC binding to SmartPass via RADIUS acct and SmartPass updates dot1x session in IF-MAP
INTRODUCING SMARTPASS CONNECT FOR BYOD

Automated, Self-Service On-Boarding

- Automatically provision client devices
  - Secure 802.1x or PSK access to the network
- Authentication:
  - Credentials (PEAP, TTLS) or Certificates (TLS)
- Automates certificate enrollment process
  - Self service client certificates deployment from Microsoft CA
- Devices:
  - iOS, Android, Windows, Mac

Client-side Reporting

- http based reporting on client state
  - Driver information, OS and platform information
# SMARTPASS CONNECT COMPONENTS

<table>
<thead>
<tr>
<th>Administrative Console</th>
<th>Wizard</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ Cloud-hosted IT provisioning utility</td>
<td>✓ Available to BYOD devices via browser:</td>
</tr>
<tr>
<td>✓ Specify configurations necessary to access the network(s)</td>
<td>✓ Automated, self-service configuration</td>
</tr>
<tr>
<td>✓ Creates deployment package for BYOD devices</td>
<td>✓ Self service certificate deployment through Microsoft CA</td>
</tr>
<tr>
<td>✓ Hosted service (SaaS) so it is always up-to-date</td>
<td>✓ When unable to connect to secure network</td>
</tr>
<tr>
<td></td>
<td>✓ Hosted on web server, in cloud, or media</td>
</tr>
</tbody>
</table>
1. New user connects to Open SSID
2. Captive portal provides link for secure network
3. SmartPass Connect configures device
4. SmartPass Connect moves device to secure SSID
SmartPass Connect allows agent-less network provisioning.

1. IT Admin configures network parameters

2. IT Admin deploys the configuration files to local web server or SmartPass server

3. User connects to open captive portal SSID and gets redirected to local web server

4. SP Connect (dissolvable) client runs through configuration on device. The dissolvable agent is downloaded to the client device and then performs config tasks

5. User device connects to secure network

6. The wizard validates connectivity to the secure SSID, uploads client details, then removes itself
JUNOS PULSE – ANYTIME, ANY DEVICE FROM ANYWHERE

Identify
- User
- Device
- Role

Onboard
- Corporate or Personal
- On Campus
- Offsite
- From Home

Manage
- Device-specific
- Ensure Adherence to Policy

Secure
- 24/7 Protection
- Anywhere
- Loss & Theft Protection
- Device Location
EMPLOYEES ON PERSONAL/COMPANY OWNED DEVICE
HOST CHECKING & APPLICATION RESTRICTION

Remote onboarding & access and the highest level of security with automatic scan for latest OS, viruses signatures, jail broken

Corporate Network

MAG Series Gateway running Junos Pulse Secure Access Service (SSL VPN)

Junos Pulse Mobile Security Suite

Scan is Clean

Complete Access

Any Device

Any Time
User downloads Junos Pulse Client from App Store

JPMSS pushes:
- VPN Profile
- WiFi Profile
- SCEP Profile

JPMSS delivers:
- 24/7 security via AV & antimalware
- MDM such as password mgmt

The device initiates a tunnel to the MAG Series Junos Pulse Gateway

Secure Access Service runs a HostCheck on the device

MAG Series Junos Pulse Gateway running Secure Access Service SSL VPN

Mobile User

Active Directory / LDAP

Data

Finance

Patch Remediation

Video

Apps

Corporate Data Center

User matched to corporate role

User has appropriate access to his role

Valid user on AD; device is OK

Secure Access authenticates the user against AD

JPMSS delivers:
- 24/7 security via AV & antimalware
- MDM such as password mgmt

JPMSS pushes:
- VPN Profile
- WiFi Profile
- SCEP Profile
JUNOS PULSE MOBILE THREAT CENTER

Worldwide 24/7 Team of Leading Security Experts

- Former Marine Computer Emergency Response Center Leadership and U.S. Coast Guard Telecommunication Specialists
- Numerous PhDs
- Certified Information Systems Security Professionals (CISSP)
- Certified Ethical Hackers (CEH), Certified Hacking Forensic Investigators (CHFI) and Certified Wireless Network Administrator (CWNA)
- Team Members in Ohio, California, Florida, Massachusetts, England, Sweden, India, Japan, etc.
MOBILE SECURITY – WHAT ARE THE THREATS?

- **Malware** – Viruses, Worms, Trojans, Spyware
- **Direct Attack** – Attacking device interfaces, Network DoS, Malicious SMS
- **Loss and Theft** – Accessing sensitive data
- **Data Communication Interception** – Sniffing data as it is transmitted and received
- **Exploitation and Misconduct** – Online predators, pornography, inappropriate communications, data leakage
First-hand research also verifies these security concerns

According to Juniper Networks Mobile Threat Center:

- Mobile malware increased 155% in 2011 and the growth continues in 2012
- Malware samples jumped 30% in the first three months of 2012
- Instances of spyware – which are designed to steal sensitive personal, financial and work information from mobile devices – have more than doubled in the first quarter of 2012 alone
MANAGE THE APPS – NOT JUST THE DEVICE

App Store

App Container

App VPN
PREPARING YOUR NETWORK FOR BYOA
APPLICATION PROLIFERATION

<table>
<thead>
<tr>
<th>Business Applications</th>
<th>Personal Applications</th>
</tr>
</thead>
</table>
| SIEBEL | ORACLE | SAP | Workday | Pivotal | Pluralsight | Sinters | Veritas | Engenius | Siemens | McKesson | Cogent 
| Epic | Cerner | Copesure | Allscripts | Naxtor | SharePoint | SAS | Price Check | Chase | CNN | Gigaom pro | ABI research | Forrester, Frost & Sullivan, Business week, Gigaom pro, ABI research

42% Increased Productivity  
39% Reduced Paperwork  
37% Increased Revenue
SOCIAL MEDIA FUNCTIONALITY IN THE ENTERPRISE

Groups, Wikis, Internal “Walls”

Profiles

Security Challenges
Up-to-date threat protection
Relevant security policies
Application visibility & control

Doc Sharing
ADDRESSING THE EVOLVING THREAT LANDSCAPE

Customer Priorities

Visibility into Web 2.0 Threats
Control of Application Usage
Rapid Response to New Threats
Scalable Policy Enforcement & Management

Juniper Security Solutions

AppSecure Software
SRX Security Service Gateways
Security Research Teams
APPSECURE: AN IMPORTANT COMPONENT TO A LAYERED SECURITY APPROACH

- Decisions made based on packet header info such as Source and Destination addresses
  - Very fast
- More context incorporated into decision process
  - Better at identifying unauthorized or forged communications
  - Still fast
- Looks at every bit for threats—thorough but intensive processing
  - Best used sparingly
APPLICATION VISIBILITY AND CONTROL IS EASY WITH APPSECURE

Application View

Firewall Enforcement

Mitigate Threats

IPS

Application Awareness and Classification Engine

What application?
What user?
User location?
User device?

Application logs sent to HQ(STRM) for reporting

Copyright © 2012 Juniper Networks, Inc. www.juniper.net
APPLICATION LEVEL FIREWALL FOR WEB 2.0 APPS

- Track which Web Applications are being consumed and how much
- Take action against the Web Applications
- Enforce security actions such as allow or deny
- Subscribe to get access to latest application signatures
- Block P2P protocols
APPSECURE SERVICE MODULES

Flow Processing

Ingress

Application Identification Engine

Egress

Application ID Results

AppTrack

IPS

AppFW

AppDoS

AppQoS
APPFW: BEYOND JUST FW OR APP CONTROL

Control & Enforce Web 2.0 Apps

- **Inspect** ports *and* protocols
- **Uncover** tunneled apps
- **Stop** multiple threat types
- **Control** nested apps, chat, file sharing and other Web 2.0 activities

Dynamic application security

Web 2.0 policy enforcement

Threat detection & prevention
BOTNET & DOS THREAT MITIGATION

AppDoS

Protect Valuable On-line Business

Detect and mitigate botnet activity

Uncover misuse of routine Web functionality

Adapt security policy and QOS based on insights

Benchmark “normal” behavior to detect anomalies

Botnet detection & remediation

DoS monitoring & remediation

On-going anomaly detection
APPQOS FOR SCALE & PERFORMANCE

Prioritize & Control App Bandwidth

Monitor Web 2.0 bandwidth consumption

Throttle bit rates based on security and usage insights

Prioritize business critical apps

Dynamic application quality-of-service (QoS)
Application prioritization
Performance management

<table>
<thead>
<tr>
<th>Applications</th>
<th>Bytes From Client (Custom) (Sum)</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>1,047,754</td>
<td>397</td>
</tr>
<tr>
<td>Windows File Share</td>
<td>1,039,016</td>
<td>134</td>
</tr>
<tr>
<td>HTTP</td>
<td>376,296</td>
<td>15</td>
</tr>
<tr>
<td>BitTorrent</td>
<td>315,064</td>
<td>15</td>
</tr>
<tr>
<td>None</td>
<td>154,150</td>
<td>152</td>
</tr>
<tr>
<td>NetSync</td>
<td>151,632</td>
<td>15</td>
</tr>
<tr>
<td>VoIP</td>
<td>128,265</td>
<td>15</td>
</tr>
<tr>
<td>Facebook</td>
<td>104,735</td>
<td>15</td>
</tr>
<tr>
<td>Telnet</td>
<td>67,920</td>
<td>15</td>
</tr>
<tr>
<td>Telnet</td>
<td>54,788</td>
<td>15</td>
</tr>
</tbody>
</table>
STRM supports SRX Series

- Intrusion Prevention System (IPS) and AppSecure
- 220+ out-of-the-box report templates
- Fully customizable reporting engine: creating, branding and scheduling delivery of reports
- Compliance reporting packages for PCI, SOX, FISMA, GLBA, and HIPAA
- Reports based on control frameworks: NIST, ISO and CoBIT
APPLE BONJOUR SERVICE IN WLAN – UNIVERSITY ENVIRONMENT

Simplicity in service sharing
- Educational institutions sharing services using Bonjour
- Students can project from their iPad to class-room Apple TV

Large campus Challenges
- 15%+ traffic related to Bonjour multicast messaging
- Does not propagate across VLANs

IT looking for device, user, location service policies
QoE data for call collected in MSFT server

‘Air quality’ monitored via each AP / WLC and collected in Campus Manager

‘Air quality’ and QoE data correlated and mashed up in CM

Lync call made from WiFi client on Juniper AP

QoE data sent from Server to CM
JUNIPER SECURITY LEADERSHIP

Market Leadership
- Data Center with High-End Firewall #1 at 54%
- Secure Mobility with SSL VPN #1 at 29%
- Intelligent Networking with Secure Routing #2 at 21%

Security Innovation
- Across Device, Network and Application
- One Junos for Routing, Switching and Security
- Security and Mobile Threat Research Teams

Proven Reach and Scale
- Protecting 76% of Smartphones Worldwide
- 24 of the Fortune 25 for Secure Connectivity
- GTM Scale with IBM, Dell, Ericsson & NSN

* Source: Infonetics Research, 4Q10
everywhere