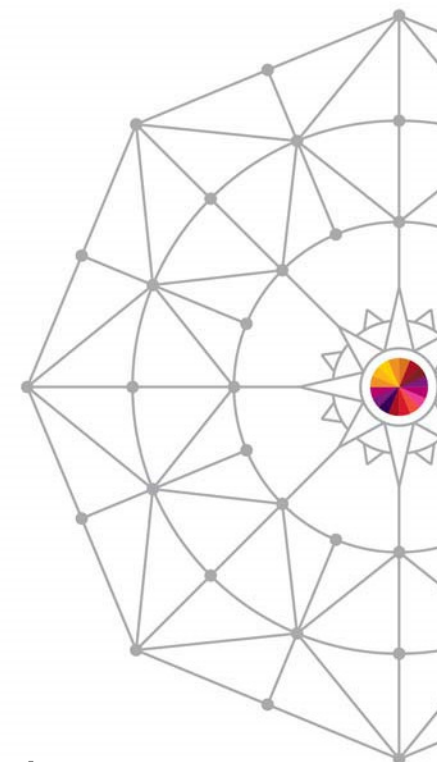


# Enterprise IPSec Deployment : A users experience



*Jim Darby: Lead System Programmer AT Nordstrom*

*Thomas Cosenza: IBM Lab Services [tcosenza@us.ibm.com](mailto:tcosenza@us.ibm.com)*

**SHARE is an independent volunteer-run information technology association that provides education, professional networking and industry influence.**

Copyright (c) 2014 by SHARE Inc.  Except where otherwise noted, this work is licensed under <http://creativecommons.org/licenses/by-nc-sa/3.0/>



# Introduction

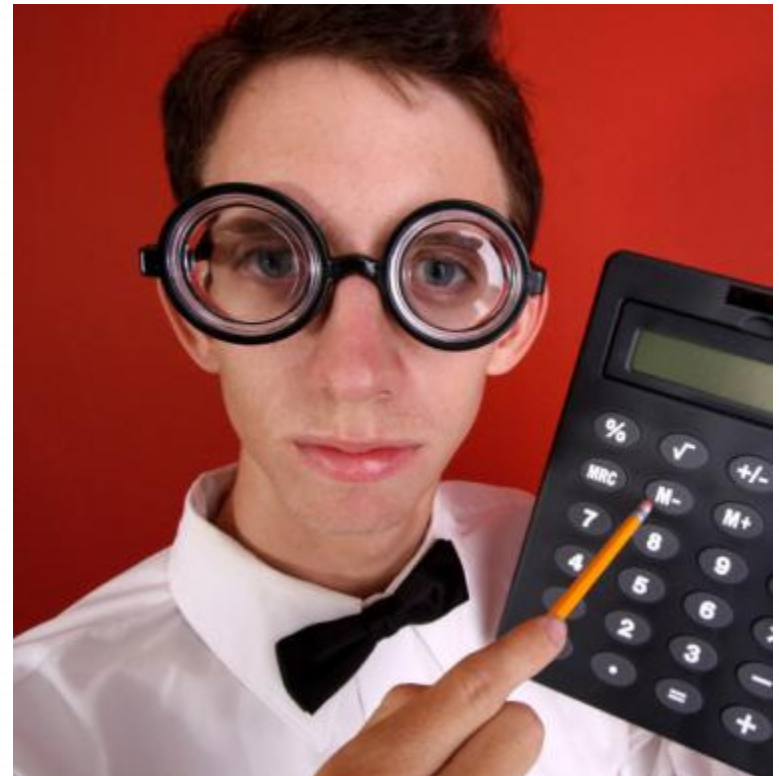
- Jim Darby
  - Jim Darby is the lead systems programmer of the IT z/OS Department at Nordstrom
  - He worked at Nordstrom for the last 28 years.
- Thomas Cosenza
  - IBM Lab Services Consultant
  - 16 years working with the Communication Server product
  - Lead z/OS IT Security consultant

# Business Problem

- In 2009 there was an internal PCI audit done
  - Requirement that all user ids and passwords needed to be encrypted to z/OS
  - TN3270 and FTP were not encrypted at the time
- There were multiple TN3270 clients that were across the organization
  - Older emulators that did not support TLS
  - Questions on how to manage all these different clients
- Lack of IP Network expertise on the z/OS staff
  - Nordstrom had a small z/OS staff which their expertise were in System management. Used communication server but did not have deep knowledge in this area

# Business Solution

- IBM Lab Services were contracted to come in and work with Nordstrom Staff
  - Immediately addresses knowledge gap
  - Allowed for “On the Job Training” with staff
  - Access to Architects and Developers in IBM through Consultant

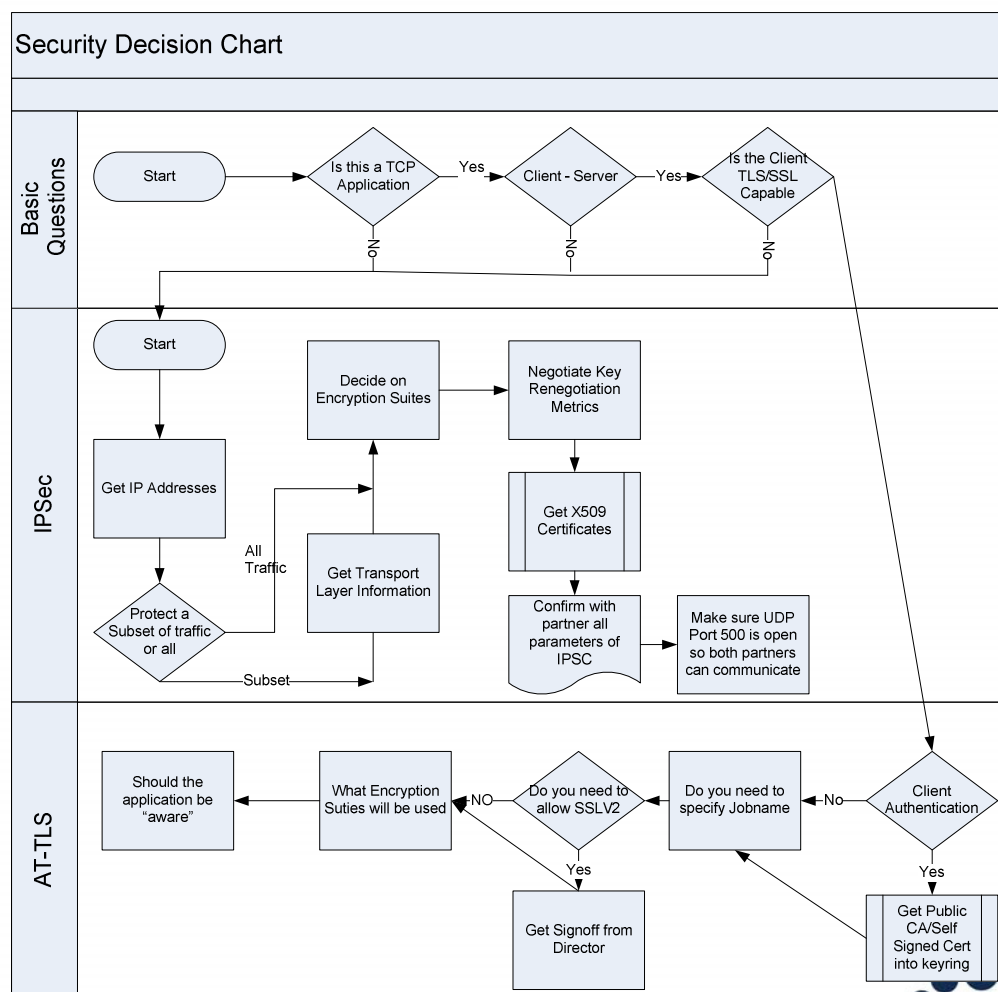


# Business Requirement

- PCI DSS compliant
- Encompass the entire Nordstrom user base
- Encrypt passwords for multiple applications to z/OS
- No large capital expenditure
  - No new software licenses
  - No new hardware purchases

# Business Solution

- Reviewing Traffic
  - Looking at Encrypting TCP applications
  - This is a Client/Server Relationship
  - Clients **NOT** TLS compatible
- Decided to use IPSec for this solution





# Review of IPSec

- **Supports many configurations**
  - Optimized for role as endpoint (host), but also support routed traffic (gateway)
  - IPSec NAT Traversal support (address translation and port translation)
  - IPv4 and IPv6 support
- **Policy-based**
  - Configuration Assistant GUI for both new and expert users
  - Direct file edit into local configuration file
- **Default filters in TCP profile provide basic protection before policy is loaded**
- **Cryptographic algorithms**
  - RSA signature-based authentication
  - ECDSA signature-based authentication (V1R12)
  - HMAC-SHA-1, HMAC-MD5 authentication
  - HMAC-SHA-2, AES-XCBC, AES-GMAC authentication (V1R12)
  - AES-CBC, 3DES and DES encryption
  - AES-GCM (128- and 256-bit) encryption (V1R12)
  - Uses cryptographic hardware if available for most algorithms
  - FIPS 140 mode (V1R12)
- **zIP Assisted IPSec**
  - Moves most IPSec processing from general purpose processors to zIPs
- **IP Security Monitoring Interface**
  - IBM Tivoli OMEGAMON XE for Mainframe Networks uses this interface
- **Support for latest IPSec RFCs**
  - RFCs 4301-4305, 4307-4308 (V1R10)
  - RFC 4306 (IKEv2) (V1R12)

# Review of IPSec

Criteria	Description
<b>From packet</b>	
Source address	Source IP address in IP header of packet
Destination address	Destination IP address in IP header of packet
Protocol	Protocol in the IP header of packet (TCP, UDP, OSPF, etc.)
Source port	For TCP and UDP, the source port in the transport header of packet
Destination port	For TCP and UDP, the destination port in the transport header of packet
ICMP type and code	For ICMP, type and code in the ICMP header of packet
OSPF type	For OSPF, type located in the OSPF header of packet
IPv6 Mobility type	For traffic with IPv6 mobility headers, MIPv6 type in header of packet.
Fragments Only	Matches fragmented packets only (applicable to routed traffic only)
<b>Network attributes</b>	
Direction	Direction of packet.
Routing	Packet is local if source or destination IP address exists on local host, otherwise it is routed
Link security class	A virtual class that allow you to group interfaces with similar security requirements. Non-VIPA addresses can be assigned a security class. Packets inherit the security class of the interface over which packet is sent/received.
<b>Time condition</b>	
Time, Day, Week, Month	Indicates when filter rule is active



# Challenge

- How to configure IPSec for Client/Server method
  - IPSec is more of a Peer to Peer solution
  - You need to identify each server with either an IP address, Hostname, FQDN, or X509DN. Can be cumbersome on a large scale
  - We can not lose the Authentication ability for each user connecting

# Business Solution

- Answer
  - Communication Server implementation allows for wild cards in Phase I identity
  - As long as the X509 Certificate on the Client has the wild carded DN name
  - The certificate also has to be signed by the trusted CA so you do not lose authentication aspect
  - **Note z/OS could not initiate the tunnel in this case**
    - This is preferred since we really want the clients to drive the connections



☐ User id @ FQDN:

☒ X.500 distinguished name:

\* ,O=Nordstrom,C=US|

## Business Solution

- The next issue was how to administer IPSec policies to all of the clients
  - Nordstrom is primarily a distributed Microsoft PC environment
- Answer (99% of user base)
  - We were able to leverage Active Directory Services
  - We pushed out IPSec policies to their user base
  - Also X509 certificates to all their users
  - Also automatically refreshes expiring certificates for client machines
- Any other platforms would be handled as a case by case bases

# Proof of Concept

- Nordstrom and IBM did a Proof of Concept for the solution
  - Needed to convert RACF commands to Top Secret; This took about a day to come up with the equivalent commands
- Learned some lessons
  - z/OS was not sending Certificate Chain
    - Caused issue with Microsoft implementation due to RFC interpretations
    - Shortened chain to just the Root CA and the Certificate
    - Fixed in later releases
  - Windows did not support AES encryption
    - Using Triple DES

# Production Deployment

- Due to time between POC to production rollout main z/OS network engineer retired
- Stage 1 – Push GPO policy but no z/OS policy
  - Our first attempt was to roll the security policy out to the clients as optional with no z/OS tunneling configured
  - Caused an immediate slow performance for all the clients coming in which we did not see in the small sample size during POC
    - Turns out the Microsoft optional policy configuration applies to each packet instead of the connection so attempted to negotiate a tunnel for each packet that was sent.
  - We had to retool our approach

# Production Deployment

- Stage 1(A)
  - This time we activated the z/OS policy server but scoped it down to a few subnets. (IT people only)
  - Through Microsoft Active Directory we only added the local IT groups
- Stage 2
  - Added all of Seattle subnets into the core z/OS / Microsoft AD policy
  - No issues at this point
- Stage 3
  - Added all subnets within Nordstrom internal network



## Issues that occurred since

- Certificate Maintenance
  - While window certificates will refresh automatically through AD policy / z/OS certificates will not.
  - Very important to refresh certificates prior to revocation
- Private key became lost
  - With the server certificate there is a separate private key.
  - The key got deleted that caused an outage
  - New certificate fixed the issue

## Current Status

- Solution is in Full affect today
  - Wildcard approach has made this a scalable solution
    - There have been 15 to 20 new stores opened however it was transparent to the IPSec policy
    - Relocated to several different corporate office buildings also with no need to change the IPSec policy
  - The solution has been in place for over 5 years now with no incidents except for issues with certificates we mentioned
  - Nordstrom is reviewing steps to move from Configuration Gui to zOSMF

# Questions





Complete your session evaluations online at [www.SHARE.org/Pittsburgh-Eval](http://www.SHARE.org/Pittsburgh-Eval)



# For more information



URL	Content
<a href="http://www.twitter.com/IBM_Commserver">http://www.twitter.com/IBM_Commserver</a> 	IBM Communications Server Twitter Feed
<a href="http://www.facebook.com/IBMCommserver">http://www.facebook.com/IBMCommserver</a> 	IBM Communications Server Facebook Fan Page
<a href="http://www.ibm.com/systems/z/">http://www.ibm.com/systems/z/</a>	IBM System z in general
<a href="http://www.ibm.com/systems/z/hardware/networking/">http://www.ibm.com/systems/z/hardware/networking/</a>	IBM Mainframe System z networking
<a href="http://www.ibm.com/software/network/commserver/">http://www.ibm.com/software/network/commserver/</a>	IBM Software Communications Server products
<a href="http://www.ibm.com/software/network/commserver/zos/">http://www.ibm.com/software/network/commserver/zos/</a>	IBM z/OS Communications Server
<a href="http://www.ibm.com/software/network/commserver/z_lin/">http://www.ibm.com/software/network/commserver/z_lin/</a>	IBM Communications Server for Linux on System z
<a href="http://www.ibm.com/software/network/ccl/">http://www.ibm.com/software/network/ccl/</a>	IBM Communication Controller for Linux on System z
<a href="http://www.ibm.com/software/network/commserver/library/">http://www.ibm.com/software/network/commserver/library/</a>	IBM Communications Server library
<a href="http://www.redbooks.ibm.com">http://www.redbooks.ibm.com</a>	ITSO Redbooks
<a href="http://www.ibm.com/software/network/commserver/zos/support/">http://www.ibm.com/software/network/commserver/zos/support/</a>	IBM z/OS Communications Server technical Support – including TechNotes from service
<a href="http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs">http://www.ibm.com/support/techdocs/atsmastr.nsf/Web/TechDocs</a>	Technical support documentation from Washington Systems Center (techdocs, flashes, presentations, white papers, etc.)
<a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a>	Request For Comments (RFC)
<a href="http://www.ibm.com/systems/z/os/zos/bkserv/">http://www.ibm.com/systems/z/os/zos/bkserv/</a>	IBM z/OS Internet library – PDF files of all z/OS manuals including Communications Server