IPv6 Security: How is the Client Secured?

Jeffrey L Carrell

Network Conversions

Network Security Consultant

IPv6 Security: How is the Client Secured?

- IPv6/IPsec
- IPsec Challenges
- IPsec Monitoring/Management Concerns
- IPsec Operations
- Microsoft SDI & DA
- Summary

IPv6/IPsec

- IPv6 standards (RFC 2460) mandate that IPsec be implemented
- The standards do not mandate that IPsec be used for all IPv6 communications
- IPsec may not be possible in small embedded devices as they may lack the computing resources to perform the encryption functions

IPsec Challenges

- The use of IPsec for every connection could be an administrative burden (some say nightmare)
- Scalability is an issue because every system must have a way to trust all other systems it will communicate with
- Many of the security problems that exist today would not exist if IPsec were more widely used
- There is not a global-scale key distribution mechanism for all systems

IPsec Monitoring/Management Concerns

- Traffic traversing the network that uses IPsec generally can not be monitored by intrusion prevention systems (IPS)
- Other network management systems may not be able to determine the protocols being used within the encrypted payload of the IPsec packets
- Some recommend IPsec to be used between sites joined by the Internet or for remote-access users, and not for use not within an organization

IPsec Operations

- IPsec can operate in either transport mode or tunnel mode
- The transport mode protects communications between hosts and it encrypts the User UDP/TCP protocol header and original data but not the IP header itself
- In tunnel mode, IPsec protects host-to-network communications like that in virtual private networks

IPsec Operations, con’t

- IPsec supports numerous authentication and encryption standards, so two IPsec-capable devices might not support the same sets of standards
- Not all devices can or will be able to support IPsec. So, before an IPsec connection can be made, whether in transport or tunnel mode, an IPsec negotiation needs to be established to determine if the IPsec supported by the two end points (host-to-host or host-to-server) are supporting the same standards

IPsec Operations, con’t

- IPsec provides security by enveloping the data (the IP payload) in an additional header or trailer that provides data origin authentication, data integrity, data confidentiality, and anti-replay protection
- The IPsec protocol uses two elements,
    - the authentication header (AH)
    - the encapsulating security payload (ESP) header and trailer
- Applying the AH or ESP to an IP datagram transforms the packet into a secure datagram. As a result, AH and ESP sometimes are referred to as transforms
- ESP is widely supported and is therefore the preferred IPsec protocol
- AH is the fallback protocol if both hosts cannot support ESP

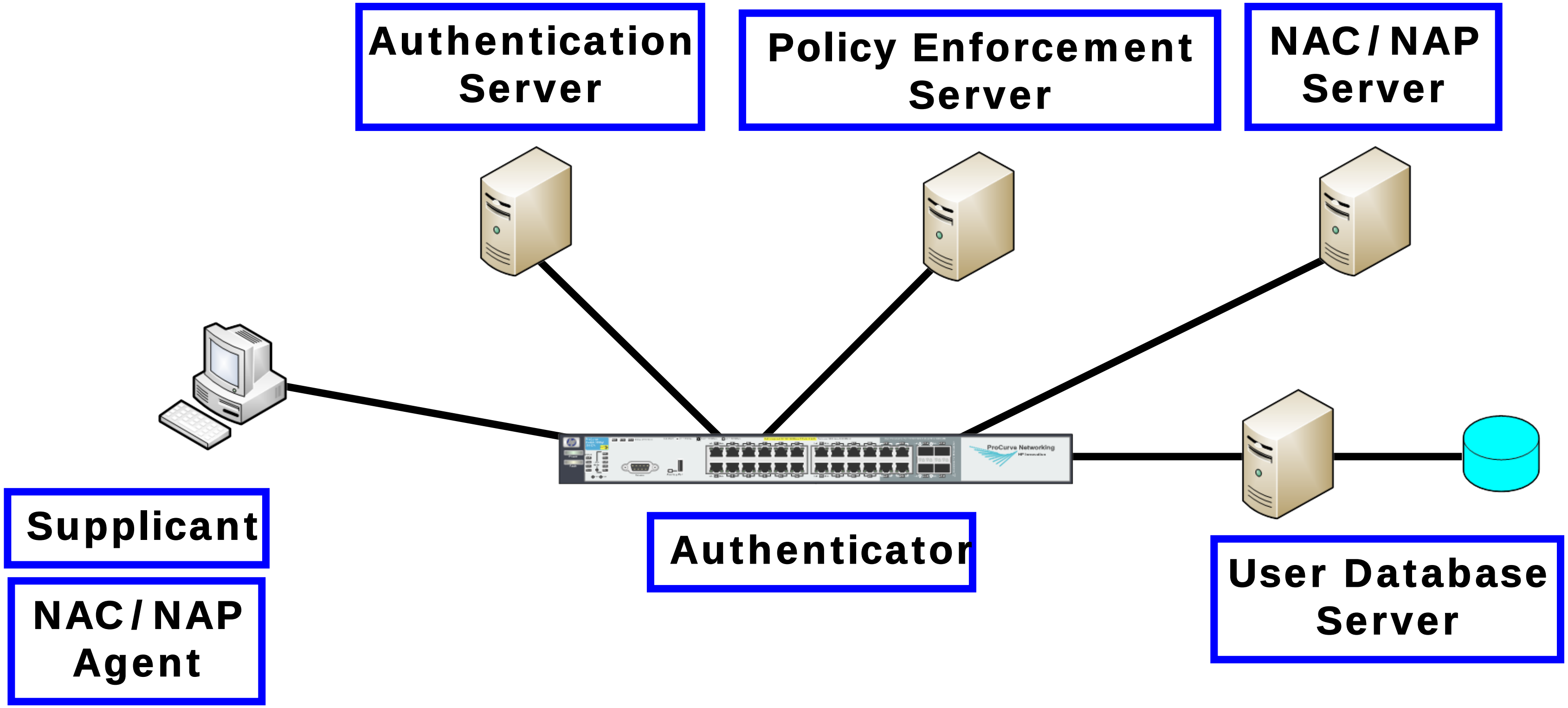
Microsoft - Server and Domain Isolation (SDI)

- SDI operates by assigning IPSec policies to the domain, via Active Directory, whereby you can create a barrier between members of the domain and all other devices
- When two devices on the domain wish to communicate, they first authenticate and all packets transferred between them are encrypted
- When a non-domain member tries to initiate communication with domain members, the authentication fails and the domain member is protected
- IPSec policies can be flexible enough to allow unsecured connections where necessary and define different requirements for different network segments and devices

Microsoft – SDI, cont’d

- SDI provides a logical barrier between the trusted network and everything else, but it is just as important to ensure that devices on the trusted network comply with the relevant security policies
- A NAC/NAP infrastructure provides an additional layer of protection by requiring hosts to comply to endpoint assessment checks (OS version, latest patches, up-to-date definitions, etc) prior to authenticating to the network as an IPsec peer
- Combining technologies like SDI with NAC/NAP can be an efficient way of securing your network

NAC/NAP System



Microsoft - DirectAccess

- DirectAccess is a way for Windows 7 clients to securely connect to the corporate network from any location without any type of traditional VPN
- DirectAccess runs over IPv6 and connects Windows 7 clients to Windows Server 2008 R2 servers
- In order for DirectAccess to communicate over the IPv4 Internet connection, bridging protocols such as ISATAP, 6to4 or Teredo will be required in order to encapsulate IPv6 packets over the IPv4 link. While these are generally transparent to the network itself, firewalls and/or routers will need to be appropriately configured for this operation

IPv6 Client Security - Summary

- Discussions around IPv6 security have centered on IPsec
- Though IPsec is mandatory in IPv6, the same issues with IPsec deployment remain from IPv4:
  - Configuration complexity & Key management
- Many IPv6 stacks do not today support IPsec, therefore, IPv6 will be deployed largely without cryptographic protections of any kind

IPv6 Client Security – Summary, con’t

- Security in IPv6 is a much broader topic than just IPsec
- IPv6 is generally enabled by default on client OS’s
  - With the additional tunnel interfaces
- Even with IPsec, there are many threats which still remain issues in IP networking

Thank You for Attending!

- Jeffrey L Carrell
- Network Security Consultant
- jeff.carrell@networkconversions.com
- jeff.carrell@ipv6hol.com